

EXHIBIT 110

**2/10/22
GOOGLE
PRIVACY
POLICY**

GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.



Privacy Checkup

Looking to change your privacy settings?

[Take the Privacy Checkup](#)

Effective February 10, 2022

[Archived versions](#)

We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads, analytics, and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web in a private mode, like Chrome Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for [key terms](#). And if you have any questions about this Privacy Policy, you can [contact us](#).

INFORMATION GOOGLE COLLECTS

We want you to understand the types of information we collect as you use our services

We collect information to provide better services to all our users – from figuring out basic stuff like which language you speak, to more complex things like which [ads you'll find most useful](#), [the people who matter most to you online](#), or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with [unique identifiers](#) tied to the browser, application, or [device](#) you're using. This allows us to do things like maintain your preferences across browsing sessions, such as your preferred language or whether to show you more relevant search results or ads based on your activity.

When you're signed in, we also collect information that we store with your Google Account, which we treat as [personal information](#).

Things you create or provide to us

When you create a Google Account, you provide us with [personal information](#) that includes your name and a password. You can also choose to add a [phone number](#) or [payment information](#) to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information – like an email address to receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

Information we collect as you use our services

Your apps, browsers & devices

We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers — for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type and carrier name, crash reports, which apps you've installed, and, depending on your device settings, other information about how you're using your Android device.

Your activity

We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

If you use our services to make and receive calls or send and receive messages, we may collect call and message log information like your phone number, calling-party number, receiving-party number, forwarding numbers, sender and recipient email address, time and date of calls and messages, duration of calls, routing information, and types and volumes of calls and messages.

You can visit your Google Account to find and manage activity information that's saved in your account.



[Go to Google Account](#)

Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions, search results for things near you, and ads based on your general location.

Your location can be determined with varying degrees of accuracy by:

- GPS and other sensor data from your device
- IP address
- Activity on Google services, such as your searches and places you label like home or work
- Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

The types of location data we collect and how long we store it depend in part on your device and account settings. For example, you can [turn your Android device's location on or off](#) using the device's settings app. You can also turn on [Location History](#) if you want to create a private map of where you go with your signed-in devices. And if your Web & App Activity setting is enabled, your searches and other activity from Google services, which may also include location information, is saved to your Google Account. Learn more about [how we use location information](#).

In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, such as directory services who provide us with business information to be displayed on

Google's services, marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertising partners to provide advertising and research services on their behalf.

We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.

WHY GOOGLE COLLECTS DATA

We use data to build better services

We use the information we collect from all our services for the following purposes:

Provide our services

We use your information to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

Maintain & improve our services

We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues that you report to us. And we use your information to make improvements to our services – for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

Develop new services

We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first photos app, helped us design and launch Google Photos.

Provide personalized services, including content and ads

We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, [Security Checkup](#) provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings.

- We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.
- We don't show you personalized ads based on your content from Drive, Gmail, or Photos.
- We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.



[Go to Ad Settings](#)

Measure performance

We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites or use apps that use Google Analytics, a Google Analytics customer may choose to enable Google to link information about your activity from that site or app with activity from other sites or apps that use our ad services.

Communicate with you

We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And

if you contact Google, we'll keep a record of your request in order to help solve any issues you might be facing.

Protect Google, our users, and the public

We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.

YOUR PRIVACY CONTROLS

You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the [Privacy Checkup](#), which provides an opportunity to review and adjust important privacy settings. In addition

to these tools, we also offer specific privacy settings in our products – you can learn more in our [Product Privacy Guide](#).



[Go to Privacy Checkup](#)

Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

We also built a place for you to review and control information saved in your Google Account. Your [Google Account](#) includes:

Privacy controls



Activity Controls

Decide what types of activity you'd like saved in your account. For example, if you have YouTube History turned on, the videos you watch and the things you search for are saved in your account so you can get better recommendations and remember where you left off. And if you have Web & App Activity turned on, your searches and activity from other Google services are saved in your account so you can get more personalized experiences like faster searches and more helpful app and content recommendations. Web & App Activity also has a subsetting that lets you control whether [information about your activity on other sites, apps, and devices that use Google services](#), such as apps you install and use on Android, is saved in your Google Account and used to improve Google services.

[Go to Activity Controls](#)



Ad settings

Manage your preferences about the ads shown to you on Google and on sites and apps that [partner with Google](#) to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

[Go to Ad Settings](#)



About you

Manage personal info in your Google Account and control who can see it across Google services.

[Go to About You](#)



Shared endorsements

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

[Go to Shared Endorsements](#)



Sites and apps that use Google services

Manage information that websites and apps using Google services, like Google Analytics, may share with Google when you visit or interact with their services.

[Go to How Google uses information from sites or apps that use our services](#)

Ways to review & update your information



My Activity

My Activity allows you to review and control data that's saved to your Google Account when you're signed in and using Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

[Go to My Activity](#)



Google Dashboard

Google Dashboard allows you to manage information associated with specific products.

[Go to Dashboard](#)

Your personal information



Manage your contact information, such as your name, email, and phone number.

[Go to Personal Info](#)

When you're signed out, you can manage information associated with your browser or device, including:

- Signed-out search personalization: [Choose](#) whether your search activity is used to offer you more relevant results and recommendations.
- YouTube settings: Pause and delete your [YouTube Search History](#) and your [YouTube Watch History](#).
- Ad Settings: [Manage](#) your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.



[Export your data](#)

You can also [request to remove content](#) from specific Google services based on applicable law.

To delete your information, you can:

- Delete your content from [specific Google services](#)
 - Search for and then delete specific items from your account using [My Activity](#)
 - [Delete specific Google products](#), including your information associated with those products
 - [Delete your entire Google Account](#)
-



[Delete your information](#)

And finally, [Inactive Account Manager](#) allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- Browser settings: For example, you can configure your browser to indicate when Google has set a [cookie](#) in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services [rely on cookies to function properly](#), for things like remembering your language preferences.
 - Device-level settings: Your device may have controls that determine what information we collect. For example, you can [modify location settings](#) on your Android device.
-

SHARING YOUR INFORMATION

When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing an app in Play, your name and photo appear next to your activity. We may also display this information in [ads depending on your Shared endorsements setting](#).

When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

With your consent

We'll share personal information outside of Google when we have your consent. For example, if you [use Google Home to make a reservation](#) through a booking service, we'll get your permission before sharing your name or phone number with the restaurant. We'll ask for your explicit consent to share any [sensitive personal information](#).

With domain administrators

If you're a student or work for an organization that uses Google services, your [domain administrator](#) and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install
- Change your account password
- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

For external processing

We provide personal information to our [affiliates](#) and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help operate our data centers, deliver our products and services, improve our internal business processes, and offer additional support to customers and users. We also use service providers to help review YouTube video content for public safety and analyze and listen to samples of saved user audio to help improve Google's audio recognition technologies.

For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, [legal process, or enforceable governmental request](#). We share information about the number and type of requests we receive from governments in our [Transparency](#)

Report.

- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.
- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

KEEPING YOUR INFORMATION SECURE

We build security into our services to protect your information

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like [Safe Browsing](#), Security Checkup, and [2 Step Verification](#) to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems

- We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.
-

EXPORTING & DELETING YOUR INFORMATION

You can export a copy of your information or delete it from your Google Account at any time

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.



[Export your data](#)

To delete your information, you can:

- Delete your content from [specific Google services](#)
 - Search for and then delete specific items from your account using [My Activity](#)
 - [Delete specific Google products](#), including your information associated with those products
 - [Delete your entire Google Account](#)
-



[Delete your information](#)

RETAINING YOUR INFORMATION

We retain the data we collect for different periods of time depending on what it is, how we use it, and how you configure your settings:

- Some data you can delete whenever you like, such as the content you create or upload. You can also delete [activity information](#) saved in your account, or [choose to have it deleted automatically](#) after a set

period of time.

- Other data is deleted or anonymized automatically after a set period of time, such as [advertising data](#) in server logs.
- We keep some data until you delete your Google Account, such as information about how often you use our services.
- And some data we retain for longer periods of time when necessary for legitimate business or legal purposes, such as security, fraud and abuse prevention, or financial record-keeping.

When you delete data, we follow a deletion process to make sure that your data is safely and completely removed from our servers or retained only in anonymized form. We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

You can read more about Google's [data retention periods](#), including how long it takes us to delete your information.

COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

Data transfers

We maintain [servers around the world](#) and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain [legal frameworks](#) relating to the transfer of data.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

California requirements

The California Consumer Privacy Act (CCPA) requires specific disclosures for California residents.

This Privacy Policy is designed to help you understand how Google handles your information:

- We explain the categories of information Google collects and the sources of that information in [Information Google collects](#).
- We explain how Google uses information in [Why Google collects data](#).
- We explain when Google may share information in [Sharing your information](#). Google does not sell your personal information.

The CCPA also provides the right to request information about how Google collects, uses, and discloses your personal information. And it gives you the right to access your information and request that Google delete that information. Finally, the CCPA provides the right to not be discriminated against for exercising your privacy rights.

We describe the choices you have to manage your privacy and data across Google's services in [Your privacy controls](#). You can exercise your rights by using these controls, which allow you to access, review, update and delete your information, as well as [export and download](#) a copy of it. When you use them, we'll validate your request by verifying that you're signed in to your Google Account. If you have questions or requests related to your rights under the CCPA, you (or your authorized agent) can also [contact Google](#). You can also find [more information](#) on Google's handling of CCPA requests.

The CCPA requires a description of data practices using specific categories. This table uses these categories to organize the information in this Privacy Policy.

Categories of personal information we collect

Identifiers such as your [name](#), [phone number](#), and address, as well as [unique identifiers](#) tied to the browser, application, or device you're using.

Demographic information, such as your [age](#), [gender](#) and [language](#).

Commercial information such as your [payment information](#) and a history of [purchases](#) you make on Google's services.

Biometric information if you choose to provide it, such as fingerprints in Google's product development [studios](#).

Internet, network, and other activity information such as your search terms; views and interactions with content and ads; Chrome browsing history you've synced with your Google Account; information about the interaction of your apps, browsers, and devices with our services (like IP address, crash reports, and system activity); and activity on third-party sites and apps that use our services. You can review and control activity data stored in your Google Account in [My Activity](#).

Geolocation data, such as may be determined by GPS, IP address, and other data from sensors on or around your device, depending in part on your device and account settings. Learn more about [Google's use of location information](#).

Audio, electronic, visual, and similar information, such as voice and audio information.

Professional, employment, and education information, such as information [you provide](#) or that is maintained through an organization using Google services at which you study or work.

Other information you create or provide, such as the content you create, upload, or receive (like photos and videos or emails, docs and spreadsheets). [Google Dashboard](#) allows you to manage information associated with specific products.

Inferences drawn from the above, like your [ads interest categories](#).

Business purposes for which information may be used or disclosed

Protecting against security threats, abuse, and illegal activity: Google uses and may disclose information to detect, prevent and respond to security incidents, and for protecting against other malicious, deceptive, fraudulent, or illegal activity. For example, to protect our services, Google may receive or disclose information about IP addresses that malicious actors have compromised.

Auditing and measurement: Google uses information for analytics and measurement to understand how our services are used, as well as to fulfill obligations to our partners like publishers, advertisers, developers, or rights holders. We may disclose non-personally identifiable information publicly and with these partners, including for auditing purposes.

Maintaining our services: Google uses information to ensure our services are working as intended, such as tracking outages or troubleshooting bugs and other issues that you report to us.

Research and development: Google uses information to improve our services and to develop new products, features and technologies that benefit our users and the public. For example, we use publicly available information to help train Google's language models and build features like Google Translate.

Use of service providers: Google shares information with service providers to perform services on our behalf, in compliance with our Privacy Policy and other appropriate confidentiality and security measures. For example, we may rely on service providers to help provide customer support.

Advertising: Google processes information to provide advertising, including online identifiers, browsing and search activity, and information about your location and interactions with advertisements. This keeps Google's services and many of the websites and services you use free of charge. You can control what information we use to show you ads by visiting your [ad settings](#).

Legal reasons: Google also uses information to satisfy applicable laws or regulations, and discloses information in response to legal process or enforceable government requests, including to law enforcement. We provide information about the number and type of requests we receive from governments in our [Transparency Report](#).

Parties with whom information may be shared

Other people with whom you choose to share your information, like docs or photos, and videos or comments on YouTube.

Third parties to whom you consent to sharing your information, such as services that integrate with Google's services. You can [review and manage third party apps and sites](#) with access to data in your Google Account.

Service providers, trusted businesses or persons that process information on Google's behalf, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

Domain administrators, if you work or study at an organization that uses Google services.

Law enforcement or other third parties, for the legal reasons described in [Sharing your information](#).

ABOUT THIS POLICY

When this policy applies

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our services
- Services offered by other companies or individuals, including products or sites they offer that may include Google services to which the policy applies, or products or sites displayed to you in search results, or linked from our services

Changes to this policy

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to [archived versions](#) for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

RELATED PRIVACY PRACTICES

Specific Google services

The following privacy notices provide additional information about some Google services:

- [Chrome & the Chrome Operating System](#)
- [Payments](#)
- [Fiber](#)
- [Google Fi](#)
- [Google Workspace for Education](#)

- [Read Along](#)
- [YouTube Kids](#)
- [Google Accounts Managed with Family Link, for Children under 13 \(or applicable age in your country\)](#)
- [Family Link privacy guide for children & teens](#)
- [Voice and Audio Collection from Children's Features on the Google Assistant](#)

If you're a member of an organization that uses Google Workspace or Google Cloud Platform, learn how these services collect and use your personal information in the [Google Cloud Privacy Notice](#).

Other useful resources

The following links highlight useful resources for you to learn more about our practices and privacy settings.

- [Your Google Account](#) is home to many of the settings you can use to manage your account
- [Privacy Checkup](#) guides you through key privacy settings for your Google Account
- [Google's safety center](#) helps you learn more about our built-in security, privacy controls, and tools to help set digital ground rules for your family online
- [Google's Teen Privacy Guide](#) provides answers to some of the top questions we get asked about privacy
- [Privacy & Terms](#) provides more context regarding this Privacy Policy and our Terms of Service
- [Technologies](#) includes more information about:
 - [How Google uses cookies](#)
 - [Technologies used for Advertising](#)
 - [How Google uses pattern recognition](#) to recognize things like faces in photos
 - [How Google uses information from sites or apps that use our services](#)

Key terms

Affiliates

An affiliate is an entity that belongs to the Google group of companies, including the following companies that provide consumer services in the EU: Google Ireland Limited, Google Commerce Ltd, Google Payment Corp, and Google Dialer Inc. Learn more about the [companies providing business services in the EU](#).

Algorithm

A process or set of rules followed by a computer in performing problem-solving operations.

Application data cache

An application data cache is a data repository on a device. It can, for example, enable a web application to run without an internet connection and improve the performance of the application by enabling faster loading of content.

Browser web storage

Browser web storage enables websites to store data in a browser on a device. When used in "local storage" mode, it enables data to be stored across sessions. This makes data retrievable even after a browser has been closed and reopened. One technology that facilitates web storage is HTML 5.

Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

Device

A device is a computer that can be used to access Google services. For example, desktop computers, tablets, smart speakers, and smartphones are all considered devices.

Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address, and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

IP address

Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. These numbers are usually assigned in geographic blocks. An IP address can often be used to identify the location from which a device is connecting to the Internet.

Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.

Personal information

This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.

Pixel tag

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is opened. Pixel tags are often used in combination with cookies.

Referrer URL

A Referrer URL (Uniform Resource Locator) is information transmitted to a destination webpage by a web browser, typically when you click a link to that page. The Referrer URL contains the URL of the last webpage the browser visited.

Sensitive personal information

This is a particular category of personal information relating to topics such as confidential medical facts, racial or ethnic origins, political or religious beliefs, or sexuality.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These “server logs” typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser.

A typical log entry for a search for “cars” looks like this:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
http://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 -
740674ce2123e969
```

- `123.45.67.89` is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.
- `25/Mar/2003 10:15:32` is the date and time of the query.
- `http://www.google.com/search?q=cars` is the requested URL, including the search query.
- `Firefox 1.0.7; Windows NT 5.1` is the browser and operating system being used.
- `740674ce2123a969` is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've visited Google, then it will be the unique cookie ID assigned to their device the next time they visit Google from that particular device).

Unique identifiers

A unique identifier is a string of characters that can be used to uniquely identify a browser, app, or device. Different identifiers vary in how permanent they are, whether they can be reset by users, and how they can be accessed.

Unique identifiers can be used for various purposes, including security and fraud detection, syncing services such as your email inbox, remembering your preferences, and providing personalized advertising. For example, unique identifiers stored in cookies help sites display content in your browser in your preferred language. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. Learn more about [how Google uses cookies](#).

On other platforms besides browsers, unique identifiers are used to recognize a specific device or app on that device. For example, a unique identifier such as the Advertising ID is used to provide relevant advertising on Android devices, and can be [managed](#) in your device's settings. Unique identifiers may also be incorporated into a device by its manufacturer (sometimes called a universally unique ID or UUID), such as the IMEI-number of a mobile phone. For example, a device's unique identifier can be used to customize our service to your device or analyze device issues related to our services.

Additional Context

ads you'll find most useful

For example, if you watch videos about baking on YouTube, you may see more ads that relate to baking as you browse the web. We also may use your IP address to determine your approximate location, so that we can serve you ads for a nearby pizza delivery service if you search for "pizza." Learn more about [Google ads](#) and [why you may see particular ads](#).

advertising and research services on their behalf

For example, advertisers may upload data from their loyalty-card programs so that they can better understand the performance of their ad campaigns. We only provide aggregated reports to advertisers that don't reveal information about individual people.

Android device with Google apps

Android devices with Google apps include devices sold by Google or one of our partners and include phones, cameras, vehicles, wearables, and televisions. These devices use Google Play Services and other pre-installed apps that include services like Gmail, Maps, your phone's camera and phone dialer, text-to-speech conversion, keyboard input, and security features. Learn more about [Google Play Services](#).

combine the information we collect

Some examples of how we combine the information we collect include:

- When you're signed in to your Google Account and search on Google, you can see search results from the public web, along with relevant information from the content you have in other Google products, like Gmail or Google Calendar. This can include things like the status of your upcoming flights, restaurant, and hotel reservations, or your photos. [Learn more](#)
- If you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name. This feature makes it easier to share things with people you know. [Learn more](#)
- The Google app can use data that you have stored in other Google products to show you personalized content, depending on your settings. For example, if you have searches stored in your Web & App Activity, the Google app can show you news articles and other information about your interests, like sports scores, based on your activity. [Learn more](#)
- If you link your Google Account to your Google Home, you can manage your information and get things done through the Google Assistant. For example, you can add events to your Google Calendar or get your schedule for the day, ask for status updates on your upcoming flight, or send information like driving directions to your phone. [Learn more](#)

customized search results

For example, when you're signed in to your Google Account and have the Web & App Activity control enabled, you can get more relevant search results that are based on your previous searches and activity from other Google services. You can [learn more here](#). You may also get customized search results even when you're signed out. If you don't want this level of search customization, you can [search and browse privately](#) or turn off [signed-out search personalization](#).

deliver our services

Examples of how we use your information to deliver our services include:

- We use the IP address assigned to your device to send you the data you requested, such as loading a YouTube video
- We use unique identifiers stored in cookies on your device to help us authenticate you as the person who should have access to your Google Account
- Photos and videos you upload to Google Photos are used to help you create albums, animations, and other creations that you can share. [Learn more](#)
- A flight confirmation email you receive may be used to create a “check-in” button that appears in your Gmail
- When you purchase services or physical goods from us, you may provide us information like your shipping address or delivery instructions. We use this information for things like processing, fulfilling, and delivering your order, and to provide support in connection with the product or service you purchase.

detect abuse

When we detect spam, malware, illegal content, and other forms of abuse on our systems in violation of our policies, we may disable your account or take other appropriate action. In certain circumstances, we may also report the violation to appropriate authorities.

devices

For example, we can use information from your devices to help you decide which device you’d like to use to install an app or view a movie you buy from Google Play. We also use this information to help protect your account.

ensure and improve

For example, we analyze how people interact with advertising to improve the performance of our ads.

ensure our services are working as intended

For example, we continuously monitor our systems to look for problems. And if we find something wrong with a specific feature, reviewing activity information collected before the problem started allows us to fix things more quickly.

Information about things near your device

If you use Google's Location services on Android, we can improve the performance of apps that rely on your location, like Google Maps. If you use Google's Location services, your device sends information to Google about its location, sensors (like accelerometer), and nearby cell towers and Wi-Fi access points (like MAC address and signal strength). All these things help to determine your location. You can use your device settings to enable Google Location services. [Learn more](#)

legal process, or enforceable governmental request

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to disclose user data. Respect for the privacy and security of data you store with Google underpins our approach to complying with these legal requests. Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process. Learn more in our [Transparency Report](#).

make improvements

For example, we use cookies to analyze how people interact with our services. And that analysis can help us build better products. For example, it may help us discover that it's taking people too long to complete a certain task or that they have trouble finishing steps at all. We can then redesign that feature and improve the product for everyone.

may link information

Google Analytics relies on first-party cookies, which means the cookies are set by the Google Analytics customer. Using our systems, data generated through Google Analytics can be linked by the Google Analytics customer and by Google to third-party cookies that are related to visits to other websites. For example, an advertiser may want to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. [Learn more](#)

partner with Google

There are over 2 million non-Google websites and apps that partner with Google to show ads. [Learn more](#)

payment information

For example, if you add a credit card or other payment method to your Google Account, you can use it to buy things across our services, like apps in the Play Store. We may also ask for other information, like a business tax ID, to help process your payment. In some cases, we may also need to verify your identity and may ask you for information to do this.

We may also use payment information to verify that you meet age requirements, if, for example, you enter an incorrect birthday indicating you're not old enough to have a Google Account. [Learn more](#)

personalized ads

You may also see personalized ads based on information from the advertiser. If you shopped on an advertiser's website, for example, they can use that visit information to show you ads. [Learn more](#)

phone number

If you add your phone number to your account, it can be used for different purposes across Google services, depending on your settings. For example, your phone number can be used to help you access your account if you forget your password, help people find and connect with you, and make the ads you see more relevant to you. [Learn more](#)

protect against abuse

For example, information about security threats can help us notify you if we think your account has been compromised (at which point we can help you take steps to protect your account).

publicly accessible sources

For example, we may collect information that's publicly available online or from other public sources to help train Google's language models and build features like Google Translate. Or, if your business's information appears on a website, we may index and display it on Google services.

rely on cookies to function properly

For example, we use a cookie called 'lbc' that makes it possible for you to open many Google Docs in one browser. Blocking this cookie would prevent Google Docs from working as expected. [Learn more](#)

safety and reliability

Some examples of how we use your information to help keep our services safe and reliable include:

- Collecting and analyzing IP addresses and cookie data to protect against automated abuse. This abuse takes many forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or censoring content by launching a Distributed Denial of Service (DDoS) attack.
- The "last account activity" feature in Gmail can help you find out if and when someone accessed your email without your knowledge. This feature shows you information about recent activity in Gmail, such as the IP addresses that accessed your mail, the associated location, and the date and time of access. [Learn more](#)

sensitive categories

When showing you personalized ads, we use topics that we think might be of interest to you based on your activity. For example, you may see ads for things like "Cooking and Recipes" or "Air Travel." We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we [require the same from advertisers](#) that use our services.

Sensor data from your device

Your device may have sensors that can be used to better understand your location and movement. For example, an accelerometer can be used to determine your speed and a gyroscope to figure out your direction of travel.

servers around the world

For example, we operate data centers located [around the world](#) to help keep our products continuously available for users.

services to make and receive calls or send and receive messages

Examples of these services include:

- Google Voice, for making and receiving calls, sending text messages, and managing voicemail
- Google Meet, for making and receiving video calls
- Gmail, for sending and receiving emails
- Google Chat, for sending and receiving messages
- Google Duo, for making and receiving video calls and sending and receiving messages
- Google Fi, for a phone plan

show trends

When lots of people start searching for something, it can provide useful information about particular trends at that time. Google Trends samples Google web searches to estimate the popularity of searches over a certain period of time and shares those results publicly in aggregated terms. [Learn more](#)

specific Google services

For example, you can delete [your blog](#) from Blogger or [a Google Site you own](#) from Google Sites. You can also delete [reviews](#) you've left on apps, games, and other content in the Play Store.

specific partners

For example, we allow YouTube creators and advertisers to work with measurement companies to learn about the audience of their YouTube videos or ads, using cookies or similar technologies. Another example is

merchants on our shopping pages, who use cookies to understand how many different people see their product listings. [Learn more](#) about these partners and how they use your information.

synced with your Google Account

Your Chrome browsing history is only saved to your account if you've enabled Chrome synchronization with your Google Account. [Learn more](#)

the people who matter most to you online

For example, when you type an address in the To, Cc, or Bcc field of an email you're composing, Gmail will suggest addresses based on the people you [contact most frequently](#).

third parties

For example, we process your information to report use statistics to rights holders about how their content was used in our services. We may also process your information if people search for your name and we display search results for sites containing publicly available information about you.

Views and interactions with content and ads

For example, we collect information about views and interactions with ads so we can provide aggregated reports to advertisers, like telling them whether we served their ad on a page and whether the ad was likely seen by a viewer. We may also measure other interactions, such as how you move your mouse over an ad or if you interact with the page on which the ad appears.

Voice and audio information

For example, you can choose whether you want Google to save an audio recording to your Google Account when you interact with Google Search, Assistant, and Maps. When your device detects an audio activation command, like "Hey Google," Google records your voice and audio plus a few seconds before the activation. [Learn more](#)

your activity on other sites and apps

This activity might come from your use of Google services, like from syncing your account with Chrome or your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your [account settings](#) and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.

[Learn more](#) about how Google uses data when you use our partners' sites or apps.

EXHIBIT 111

**10/4/22
GOOGLE
PRIVACY
POLICY**

GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.



Privacy Checkup

Looking to change your privacy settings?

[Take the Privacy Checkup](#)

Effective October 4, 2022

[Archived versions](#)

We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads, analytics, and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web in a private mode, like Chrome Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for [key terms](#). And if you have any questions about this Privacy Policy, you can [contact us](#).

INFORMATION GOOGLE COLLECTS

We want you to understand the types of information we collect as you use our services

We collect information to provide better services to all our users — from figuring out basic stuff like which language you speak, to more complex things like which [ads you'll find most useful](#), [the people who matter most to you online](#), or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with [unique identifiers](#) tied to the browser, application, or device you're using. This allows us to do things like maintain your preferences across browsing sessions, such as your preferred language or whether to show you more relevant search results or ads based on your activity.

When you're signed in, we also collect information that we store with your Google Account, which we treat as [personal information](#).

Things you create or provide to us

When you create a Google Account, you provide us with [personal information](#) that includes your name and a password. You can also choose to add a [phone number](#) or [payment information](#) to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information — like an email address to communicate with Google or receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

Information we collect as you use our services

Your apps, browsers & devices

We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers — for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type and carrier name, crash reports, which apps you've installed, and, depending on your device settings, other information about how you're using your Android device.

Your activity

We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information
- Purchase activity

- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

If you use our services to make and receive calls or send and receive messages, we may collect call and message log information like your phone number, calling-party number, receiving-party number, forwarding numbers, sender and recipient email address, time and date of calls and messages, duration of calls, routing information, and types and volumes of calls and messages.

You can visit your Google Account to find and manage activity information that's saved in your account.



[Go to Google Account](#)

Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions, search results for things near you, and ads based on your general location.

Your location can be determined with varying degrees of accuracy by:

- GPS and other sensor data from your device
- IP address
- Activity on Google services, such as your searches and places you label like home or work
- Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

The types of location data we collect and how long we store it depend in part on your device and account settings. For example, you can turn your Android device's location on or off using the device's settings app. You can also turn on Location History if you want to create a private map of where you go with your signed-in devices. And if your Web & App Activity setting is enabled, your

searches and other activity from Google services, which may also include location information, is saved to your Google Account. Learn more about [how we use location information](#).

In some circumstances, Google also collects information about you from [publicly accessible sources](#). For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, such as directory services who provide us with business information to be displayed on Google's services, marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to [protect against abuse](#). We also receive information from advertising partners to provide [advertising and research services on their behalf](#).

We use various technologies to collect and store information, including [cookies](#), [pixel tags](#), local storage, such as [browser web storage](#) or [application data caches](#), databases, and [server logs](#).

WHY GOOGLE COLLECTS DATA

We use data to build better services

We use the information we collect from all our services for the following purposes:

Provide our services

We use your information to [deliver our services](#), like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

Maintain & improve our services

We also use your information to [ensure our services are working as intended](#), such as tracking outages or troubleshooting issues that you report to us. And we use your information to [make improvements](#) to our services – for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

Develop new services

We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first photos app, helped us design and launch Google Photos.

Provide personalized services, including content and ads

We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, [Security Checkup](#) provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for "mountain bikes," you may see an ad for sports equipment when you're browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings.

- We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.
- We don't show you personalized ads based on your content from Drive, Gmail, or Photos.
- We don't share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the "tap to call" button, we'll connect your call and may share your phone number with the flower shop.



[Go to Ad Settings](#)

Measure performance

We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites or use apps that use Google Analytics, a Google Analytics customer may choose to enable Google to link information about your activity from that site or app with activity from other sites or apps that use our ad services.

Communicate with you

We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And if you contact Google, we'll keep a record of your request in order to help solve any issues you might be facing.

Protect Google, our users, and the public

We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.

YOUR PRIVACY CONTROLS

You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the [Privacy Checkup](#), which provides an opportunity to review and adjust important privacy settings. In addition to these tools, we also offer specific privacy settings in our products — you can learn more in our [Product Privacy Guide](#).



[Go to Privacy Checkup](#)

Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

We also built a place for you to review and control information saved in your Google Account. Your [Google Account](#) includes:

Privacy controls



Activity Controls

Decide what types of activity you'd like saved in your account. For example, if you have YouTube History turned on, the videos you watch and the things you search for are saved in your account so you can get better recommendations and remember where you left off. And if you have Web & App Activity turned on, your searches and activity from other Google services are saved in your account so you can get more personalized experiences like faster searches and more helpful app and content recommendations. Web & App Activity also has a subsetting that lets you control whether [information about your activity on other sites, apps, and devices that use Google services](#), such as apps you install and use on Android, is saved in your Google Account and used to improve Google services.

[Go to Activity Controls](#)



Ad settings

Manage your preferences about the ads shown to you on Google and on sites and apps that [partner with Google](#) to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

[Go to Ad Settings](#)



About you

Manage personal info in your Google Account and control who can see it across Google services.

[Go to About You](#)



Shared endorsements

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

[Go to Shared Endorsements](#)



Sites and apps that use Google services

Manage information that websites and apps using Google services, like Google Analytics, may share with Google when you visit or interact with their services.

[Go to How Google uses information from sites or apps that use our services](#)

Ways to review & update your information



My Activity

My Activity allows you to review and control data that's saved to your Google Account when you're signed in and using Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

[Go to My Activity](#)



Google Dashboard

Google Dashboard allows you to manage information associated with specific products.

[Go to Dashboard](#)



Your personal information

Manage your contact information, such as your name, email, and phone number.

[Go to Personal Info](#)

When you're signed out, you can manage information associated with your browser or device, including:

- Signed-out search personalization: [Choose](#) whether your search activity is used to offer you more relevant results and recommendations.
- YouTube settings: Pause and delete your [YouTube Search History](#) and your [YouTube Watch History](#).
- Ad Settings: [Manage](#) your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.



[Export your data](#)

To delete your information, you can:

- Delete your content from [specific Google services](#)
- Search for and then delete specific items from your account using [My Activity](#)
- [Delete specific Google products](#), including your information associated with those products
- [Delete your entire Google Account](#)



[Delete your information](#)

[Inactive Account Manager](#) allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

And finally, you can also [request to remove content](#) from specific Google services based on applicable law and our policies.

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- Browser settings: For example, you can configure your browser to indicate when Google has set a [cookie](#) in your browser. You can also configure your browser to block all cookies from a

specific domain or all domains. But remember that our services rely on cookies to function properly, for things like remembering your language preferences.

- Device-level settings: Your device may have controls that determine what information we collect. For example, you can [modify location settings](#) on your Android device.
-

SHARING YOUR INFORMATION

When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing an app in Play, your name and photo appear next to your activity. We may also display this information in [ads depending on your Shared endorsements setting](#).

When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

With your consent

We'll share personal information outside of Google when we have your consent. For example, if you [use Google Home to make a reservation](#) through a booking service, we'll get your permission before sharing your name or phone number with the restaurant. We also provide you with controls to [review and manage third party apps and sites](#) you have given access to data in your Google Account. We'll ask for your explicit consent to share any sensitive personal information.

With domain administrators

If you're a student or work for an organization that uses Google services, your [domain administrator](#) and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install
- Change your account password
- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

For external processing

We provide personal information to our [affiliates](#) and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help operate our data centers, deliver our products and services, improve our internal business processes, and offer additional support to customers and users. We also use service providers to help review YouTube video content for public safety and analyze and listen to samples of saved user audio to help improve Google's audio recognition technologies.

For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, [legal process](#), or [enforceable governmental request](#). We share information about the number and type of requests we receive from governments in our [Transparency Report](#).
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.

- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners – like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

KEEPING YOUR INFORMATION SECURE

We build security into our services to protect your information

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like [Safe Browsing](#), Security Checkup, and [2 Step Verification](#) to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict

contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.

EXPORTING & DELETING YOUR INFORMATION

You can export a copy of your information or delete it from your Google Account at any time

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.



[Export your data](#)

To delete your information, you can:

- Delete your content from [specific Google services](#)
 - Search for and then delete specific items from your account using [My Activity](#)
 - [Delete specific Google products](#), including your information associated with those products
 - [Delete your entire Google Account](#)
-



[Delete your information](#)

RETAINING YOUR INFORMATION

We retain the data we collect for different periods of time depending on what it is, how we use it, and how you configure your settings:

- Some data you can delete whenever you like, such as your [personal info](#) or the content you create or upload, like [photos](#) and [documents](#). You can also delete [activity information](#) saved in

your account, or [choose to have it deleted automatically](#) after a set period of time. We'll keep this data in your Google Account until you remove it or choose to have it removed.

- Other data is deleted or anonymized automatically after a set period of time, such as [advertising data](#) in server logs.
- We keep some data until you delete your Google Account, such as information about how often you use our services.
- And some data we retain for longer periods of time when necessary for legitimate business or legal purposes, such as security, fraud and abuse prevention, or financial record-keeping.

When you delete data, we follow a deletion process to make sure that your data is safely and completely removed from our servers or retained only in anonymized form. We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

You can read more about Google's [data retention periods](#), including how long it takes us to delete your information.

COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

Data transfers

We maintain [servers around the world](#) and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain [legal frameworks](#) relating to the transfer of data.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection

authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

California requirements

The California Consumer Privacy Act (CCPA) requires specific disclosures for California residents.

This Privacy Policy is designed to help you understand how Google handles your information:

- We explain the categories of information Google collects and the sources of that information in [Information Google collects](#).
- We explain how Google uses information in [Why Google collects data](#).
- We explain when Google may share information in [Sharing your information](#). Google does not sell your personal information.

The CCPA also provides the right to request information about how Google collects, uses, and discloses your personal information. And it gives you the right to access your information and request that Google delete that information. Finally, the CCPA provides the right to not be discriminated against for exercising your privacy rights.

We describe the choices you have to manage your privacy and data across Google's services in [Your privacy controls](#). You can exercise your rights by using these controls, which allow you to access, review, update and delete your information, as well as [export and download](#) a copy of it. When you use them, we'll validate your request by verifying that you're signed in to your Google Account. If you have questions or requests related to your rights under the CCPA, you (or your authorized agent) can also [contact Google](#). You can also find [more information](#) on Google's handling of CCPA requests.

The CCPA requires a description of data practices using specific categories. This table uses these categories to organize the information in this Privacy Policy.

Categories of personal information we collect

Identifiers such as your [name](#), [phone number](#), and address, as well as [unique identifiers](#) tied to the browser, application, or device you're using.

Demographic information, such as your [age](#), [gender](#) and [language](#).

Commercial information such as your [payment information](#) and a history of [purchases](#) you make on Google's services.

Biometric information if you choose to provide it, such as fingerprints in Google's product development studies.

Internet, network, and other activity information such as your search terms; views and interactions with content and ads; Chrome browsing history you've synced with your Google Account; information about the interaction of your apps, browsers, and devices with our services (like IP address, crash reports, and system activity); and activity on third-party sites and apps that use our services. You can review and control activity data stored in your Google Account in [My Activity](#).

Geolocation data, such as may be determined by GPS, IP address, and other data from sensors on or around your device, depending in part on your device and account settings. Learn more about [Google's use of location information](#).

Audio, electronic, visual, and similar information, such as [voice and audio information](#).

Professional, employment, and education information, such as information [you provide](#) or that is maintained through an organization using Google services at which you study or work.

Other information you create or provide, such as the content you create, upload, or receive (like photos and videos or emails, docs and spreadsheets). [Google Dashboard](#) allows you to manage information associated with specific products.

Inferences drawn from the above, like your [ads interest categories](#).

Business purposes for which information may be used or disclosed

Protecting against security threats, abuse, and illegal activity: Google uses and may disclose information to detect, prevent and respond to security incidents, and for protecting against other malicious, deceptive, fraudulent, or illegal activity. For example, to protect our services, Google may receive or disclose information about IP addresses that malicious actors have compromised.

Auditing and measurement: Google uses information for analytics and measurement to understand how our services are used, as well as to fulfill obligations to our partners like publishers, advertisers, developers, or rights holders. We may disclose non-personally identifiable information publicly and with these partners, including for auditing purposes.

Maintaining our services: Google uses information to ensure our services are working as intended, such as tracking outages or troubleshooting bugs and other issues that you report to us.

Research and development: Google uses information to improve our services and to develop new products, features and technologies that benefit our users and the public. For example, we use publicly available information to help train Google's language models and build features like Google Translate.

Use of service providers: Google shares information with service providers to perform services on our behalf, in compliance with our Privacy Policy and other appropriate confidentiality and security measures. For example, we may rely on service providers to help provide customer support.

Advertising: Google processes information to provide advertising, including online identifiers, browsing and search activity, and information about your location and interactions with advertisements. This keeps Google's services and many of the websites and services you use free of charge. You can control what information we use to show you ads by visiting your [ad settings](#).

Legal reasons: Google also uses information to satisfy applicable laws or regulations, and discloses information in response to legal process or enforceable government requests, including to law enforcement. We provide information about the number and type of requests we receive from governments in our [Transparency Report](#).

Parties with whom information may be shared

Other people with whom you choose to share your information, like docs or photos, and videos or comments on YouTube.

Third parties to whom you consent to sharing your information, such as services that integrate with Google's services. You can [review and manage third party apps and sites](#) with access to data in your

Google Account.

Service providers, trusted businesses or persons that process information on Google's behalf, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

Domain administrators, if you work or study at an organization that uses Google services.

Law enforcement or other third parties, for the legal reasons described in [Sharing your information](#).

ABOUT THIS POLICY

When this policy applies

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our services
- Services offered by other companies or individuals, including products or sites they offer that may include Google services to which the policy applies, or products or sites displayed to you in search results, or linked from our services

Changes to this policy

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to [archived versions](#) for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

RELATED PRIVACY PRACTICES

Specific Google services

The following privacy notices provide additional information about some Google services:

- [Chrome & the Chrome Operating System](#)
- [Payments](#)
- [Fiber](#)
- [Google Fi](#)
- [Google Workspace for Education](#)
- [Read Along](#)
- [YouTube Kids](#)
- [Google Accounts Managed with Family Link, for Children under 13 \(or applicable age in your country\)](#)
- [Family Link privacy guide for children & teens](#)
- [Voice and Audio Collection from Children's Features on the Google Assistant](#)

If you're a member of an organization that uses Google Workspace or Google Cloud Platform, learn how these services collect and use your personal information in the [Google Cloud Privacy Notice](#).

Other useful resources

The following links highlight useful resources for you to learn more about our practices and privacy settings.

- [Your Google Account](#) is home to many of the settings you can use to manage your account
- [Privacy Checkup](#) guides you through key privacy settings for your Google Account

- [Google's safety center](#) helps you learn more about our built-in security, privacy controls, and tools to help set digital ground rules for your family online
 - [Google's Teen Privacy Guide](#) provides answers to some of the top questions we get asked about privacy
 - [Privacy & Terms](#) provides more context regarding this Privacy Policy and our Terms of Service
 - [Technologies](#) includes more information about:
 - [How Google uses cookies](#)
 - Technologies used for [Advertising](#)
 - [How Google uses pattern recognition](#) to recognize things like faces in photos
 - [How Google uses information from sites or apps that use our services](#)
-

Key terms

Affiliates

An affiliate is an entity that belongs to the Google group of companies, including the following companies that provide consumer services in the EU: Google Ireland Limited, Google Commerce Ltd, Google Payment Corp, and Google Dialer Inc. Learn more about the [companies providing business services in the EU](#).

Algorithm

A process or set of rules followed by a computer in performing problem-solving operations.

Application data cache

An application data cache is a data repository on a device. It can, for example, enable a web application to run without an internet connection and improve the performance of the application by

enabling faster loading of content.

Browser web storage

Browser web storage enables websites to store data in a browser on a device. When used in "local storage" mode, it enables data to be stored across sessions. This makes data retrievable even after a browser has been closed and reopened. One technology that facilitates web storage is HTML 5.

Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

Device

A device is a computer that can be used to access Google services. For example, desktop computers, tablets, smart speakers, and smartphones are all considered devices.

Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address, and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

IP address

Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. These numbers are usually assigned in geographic blocks. An IP address can often be used

to identify the location from which a device is connecting to the Internet.

Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.

Personal information

This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.

Pixel tag

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is opened. Pixel tags are often used in combination with cookies.

Referrer URL

A Referrer URL (Uniform Resource Locator) is information transmitted to a destination webpage by a web browser, typically when you click a link to that page. The Referrer URL contains the URL of the last webpage the browser visited.

Sensitive personal information

This is a particular category of personal information relating to topics such as confidential medical facts, racial or ethnic origins, political or religious beliefs, or sexuality.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These “server logs” typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser.

A typical log entry for a search for “cars” looks like this:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
http://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 -
740674ce2123e969
```

- `123.45.67.89` is the Internet Protocol address assigned to the user by the user's ISP. Depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet.
- `25/Mar/2003 10:15:32` is the date and time of the query.
- `http://www.google.com/search?q=cars` is the requested URL, including the search query.
- `Firefox 1.0.7; Windows NT 5.1` is the browser and operating system being used.
- `740674ce2123a969` is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they've visited Google, then it will be the unique cookie ID assigned to their device the next time they visit Google from that particular device).

Unique identifiers

A unique identifier is a string of characters that can be used to uniquely identify a browser, app, or device. Different identifiers vary in how permanent they are, whether they can be reset by users, and how they can be accessed.

Unique identifiers can be used for various purposes, including security and fraud detection, syncing services such as your email inbox, remembering your preferences, and providing personalized advertising. For example, unique identifiers stored in cookies help sites display content in your browser in your preferred language. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. Learn more about [how Google uses cookies](#).

On other platforms besides browsers, unique identifiers are used to recognize a specific device or app on that device. For example, a unique identifier such as the Advertising ID is used to provide relevant advertising on Android devices, and can be [managed](#) in your device's settings. Unique identifiers may also be incorporated into a device by its manufacturer (sometimes called a universally unique ID or UUID), such as the IMEI-number of a mobile phone. For example, a device's unique identifier can be used to customize our service to your device or analyze device issues related to our services.

Additional Context

ads you'll find most useful

For example, if you watch videos about baking on YouTube, you may see more ads that relate to baking as you browse the web. We also may use your IP address to determine your approximate location, so that we can serve you ads for a nearby pizza delivery service if you search for "pizza." Learn more [about Google ads](#) and [why you may see particular ads](#).

advertising and research services on their behalf

For example, advertisers may upload data from their loyalty-card programs so that they can better understand the performance of their ad campaigns. We only provide aggregated reports to advertisers that don't reveal information about individual people.

Android device with Google apps

Android devices with Google apps include devices sold by Google or one of our partners and include phones, cameras, vehicles, wearables, and televisions. These devices use Google Play Services and other pre-installed apps that include services like Gmail, Maps, your phone's camera and phone dialer, text-to-speech conversion, keyboard input, and security features. Learn more about [Google Play Services](#).

combine the information we collect

Some examples of how we combine the information we collect include:

- When you're signed in to your Google Account and search on Google, you can see search results from the public web, along with relevant information from the content you have in other Google products, like Gmail or Google Calendar. This can include things like the status of your upcoming flights, restaurant, and hotel reservations, or your photos. [Learn more](#)
- If you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name. This feature makes it easier to share things with people you know. [Learn more](#)
- The Google app can use data that you have stored in other Google products to show you personalized content, depending on your settings. For example, if you have searches stored in your Web & App Activity, the Google app can show you news articles and other information about your interests, like sports scores, based your activity. [Learn more](#)
- If you link your Google Account to your Google Home, you can manage your information and get things done through the Google Assistant. For example, you can add events to your Google Calendar or get your schedule for the day, ask for status updates on your upcoming flight, or send information like driving directions to your phone. [Learn more](#)

customized search results

For example, when you're signed in to your Google Account and have the Web & App Activity control enabled, you can get more relevant search results that are based on your previous searches and activity from other Google services. You can [learn more here](#). You may also get customized search results even when you're signed out. If you don't want this level of search customization, you can [search and browse privately](#) or turn off [signed-out search personalization](#).

deliver our services

Examples of how we use your information to deliver our services include:

- We use the IP address assigned to your device to send you the data you requested, such as loading a YouTube video
- We use unique identifiers stored in cookies on your device to help us authenticate you as the person who should have access to your Google Account

- Photos and videos you upload to Google Photos are used to help you create albums, animations, and other creations that you can share. [Learn more](#)
- A flight confirmation email you receive may be used to create a “check-in” button that appears in your Gmail
- When you purchase services or physical goods from us, you may provide us information like your shipping address or delivery instructions. We use this information for things like processing, fulfilling, and delivering your order, and to provide support in connection with the product or service you purchase.

detect abuse

When we detect spam, malware, illegal content, and other forms of abuse on our systems in violation of our policies, we may disable your account or take other appropriate action. In certain circumstances, we may also report the violation to appropriate authorities.

devices

For example, we can use information from your devices to help you decide which device you’d like to use to install an app or view a movie you buy from Google Play. We also use this information to help protect your account.

ensure and improve

For example, we analyze how people interact with advertising to improve the performance of our ads.

ensure our services are working as intended

For example, we continuously monitor our systems to look for problems. And if we find something wrong with a specific feature, reviewing activity information collected before the problem started allows us to fix things more quickly.

Information about things near your device

If you use Google's Location services on Android, we can improve the performance of apps that rely on your location, like Google Maps. If you use Google's Location services, your device sends information to Google about its location, sensors (like accelerometer), and nearby cell towers and Wi-Fi access points (like MAC address and signal strength). All these things help to determine your location. You can use your device settings to enable Google Location services. [Learn more](#)

legal process, or enforceable governmental request

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to disclose user data. Respect for the privacy and security of data you store with Google underpins our approach to complying with these legal requests. Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process. Learn more in our [Transparency Report](#).

make improvements

For example, we use cookies to analyze how people interact with our services. And that analysis can help us build better products. For example, it may help us discover that it's taking people too long to complete a certain task or that they have trouble finishing steps at all. We can then redesign that feature and improve the product for everyone.

may link information

Google Analytics relies on first-party cookies, which means the cookies are set by the Google Analytics customer. Using our systems, data generated through Google Analytics can be linked by the Google Analytics customer and by Google to third-party cookies that are related to visits to other websites. For example, an advertiser may want to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. [Learn more](#)

our users

For example, to prevent abuse and increase transparency and accountability over our online content moderation practices, Google shares data about requests for removal of content from our services with Lumen, which collects and analyzes these requests to facilitate research to help Internet users understand their rights. [Learn more](#).

partner with Google

There are over 2 million non-Google websites and apps that partner with Google to show ads. [Learn more](#)

payment information

For example, if you add a credit card or other payment method to your Google Account, you can use it to buy things across our services, like apps in the Play Store. We may also ask for other information, like a business tax ID, to help process your payment. In some cases, we may also need to verify your identity and may ask you for information to do this.

We may also use payment information to verify that you meet age requirements, if, for example, you enter an incorrect birthday indicating you're not old enough to have a Google Account. [Learn more](#)

personalized ads

You may also see personalized ads based on information from the advertiser. If you shopped on an advertiser's website, for example, they can use that visit information to show you ads. [Learn more](#)

phone number

If you add your phone number to your account, it can be used for different purposes across Google services, depending on your settings. For example, your phone number can be used to help you access your account if you forget your password, help people find and connect with you, and make the ads you see more relevant to you. [Learn more](#)

protect against abuse

For example, information about security threats can help us notify you if we think your account has been compromised (at which point we can help you take steps to protect your account).

publicly accessible sources

For example, we may collect information that's publicly available online or from other public sources to help train Google's language models and build features like Google Translate. Or, if your business's information appears on a website, we may index and display it on Google services.

rely on cookies to function properly

For example, we use a cookie called 'lbc' that makes it possible for you to open many Google Docs in one browser. Blocking this cookie would prevent Google Docs from working as expected. [Learn more](#)

safety and reliability

Some examples of how we use your information to help keep our services safe and reliable include:

- Collecting and analyzing IP addresses and cookie data to protect against automated abuse. This abuse takes many forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or censoring content by launching a Distributed Denial of Service (DDoS) attack.
- The "last account activity" feature in Gmail can help you find out if and when someone accessed your email without your knowledge. This feature shows you information about recent activity in Gmail, such as the IP addresses that accessed your mail, the associated location, and the date and time of access. [Learn more](#)

sensitive categories

When showing you personalized ads, we use topics that we think might be of interest to you based on your activity. For example, you may see ads for things like "Cooking and Recipes" or "Air Travel." We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we [require the same from advertisers](#) that use our services.

Sensor data from your device

Your device may have sensors that can be used to better understand your location and movement. For example, an accelerometer can be used to determine your speed and a gyroscope to figure out your direction of travel.

servers around the world

For example, we operate data centers located [around the world](#) to help keep our products continuously available for users.

services to make and receive calls or send and receive messages

Examples of these services include:

- Google Voice, for making and receiving calls, sending text messages, and managing voicemail
- Google Meet, for making and receiving video calls
- Gmail, for sending and receiving emails
- Google Chat, for sending and receiving messages
- Google Duo, for making and receiving video calls and sending and receiving messages
- Google Fi, for a phone plan

show trends

When lots of people start searching for something, it can provide useful information about particular trends at that time. Google Trends samples Google web searches to estimate the popularity of searches over a certain period of time and shares those results publicly in aggregated terms. [Learn more](#)

specific Google services

For example, you can delete [your blog](#) from Blogger or [a Google Site you own](#) from Google Sites. You can also delete [reviews](#) you've left on apps, games, and other content in the Play Store.

specific partners

For example, we allow YouTube creators and advertisers to work with measurement companies to learn about the audience of their YouTube videos or ads, using cookies or similar technologies. Another example is merchants on our shopping pages, who use cookies to understand how many different people see their product listings. [Learn more](#) about these partners and how they use your information.

synced with your Google Account

Your Chrome browsing history is only saved to your account if you've enabled Chrome synchronization with your Google Account. [Learn more](#)

the people who matter most to you online

For example, when you type an address in the To, Cc, or Bcc field of an email you're composing, Gmail will suggest addresses based on the people you [contact most frequently](#).

the public

For example, we process information about [requests to remove content](#) from our services under Google's content removal policies or applicable law to assess the request, and to ensure transparency, improve accountability and prevent abuse and fraud in these practices.

third parties

For example, we process your information to report use statistics to rights holders about how their content was used in our services. We may also process your information if people search for your name and we display search results for sites containing publicly available information about you.

Views and interactions with content and ads

For example, we collect information about views and interactions with ads so we can provide aggregated reports to advertisers, like telling them whether we served their ad on a page and whether the ad was likely seen by a viewer. We may also measure other interactions, such as how you move your mouse over an ad or if you interact with the page on which the ad appears.

Voice and audio information

For example, you can choose whether you want Google to save an audio recording to your Google Account when you interact with Google Search, Assistant, and Maps. When your device detects an audio activation command, like “Hey Google,” Google records your voice and audio plus a few seconds before the activation. [Learn more](#)

your activity on other sites and apps

This activity might come from your use of Google services, like from syncing your account with Chrome or your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your [account settings](#) and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.

[Learn more](#) about how Google uses data when you use our partners' sites or apps.

EXHIBIT 112

**12/15/22
GOOGLE
PRIVACY
POLICY**

GOOGLE PRIVACY POLICY

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.

This Privacy Policy is meant to help you understand what information we collect, why we collect it, and how you can update, manage, export, and delete your information.



Privacy Checkup

Looking to change your privacy settings?

[Take the Privacy Checkup](#)

Effective December 15, 2022

[Archived versions](#)

We build a range of services that help millions of people daily to explore and interact with the world in new ways. Our services include:

- Google apps, sites, and devices, like Search, YouTube, and Google Home
- Platforms like the Chrome browser and Android operating system
- Products that are integrated into third-party apps and sites, like ads, analytics, and embedded Google Maps

You can use our services in a variety of ways to manage your privacy. For example, you can sign up for a Google Account if you want to create and manage content like emails and photos, or see more relevant search results. And you can use many Google services when you're signed out or without creating an account at all, like searching on Google or watching YouTube videos. You can also choose to browse the web in a private mode, like Chrome Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.

To help explain things as clearly as possible, we've added examples, explanatory videos, and definitions for [key terms](#). And if you have any questions about this Privacy Policy, you can [contact us](#).

INFORMATION GOOGLE COLLECTS

We want you to understand the types of information we collect as you use our services

We collect information to provide better services to all our users – from figuring out basic stuff like which language you speak, to more complex things like which [ads you'll find most useful](#), [the people who matter most to you online](#), or which YouTube videos you might like. The information Google collects, and how that information is used, depends on how you use our services and how you manage your privacy controls.

When you're not signed in to a Google Account, we store the information we collect with [unique identifiers](#) tied to the browser, application, or [device](#) you're using. This allows us to do things like maintain your preferences across browsing sessions, such as your preferred language or whether to show you more relevant search results or ads based on your activity.

When you're signed in, we also collect information that we store with your Google Account, which we treat as [personal information](#).

Things you create or provide to us

When you create a Google Account, you provide us with [personal information](#) that includes your name and a password. You can also choose to add a [phone number](#) or [payment information](#) to your account. Even if you aren't signed in to a Google Account, you might choose to provide us with information – like an email address to communicate with Google or receive updates about our services.

We also collect the content you create, upload, or receive from others when using our services. This includes things like email you write and receive, photos and videos you save, docs and spreadsheets you create, and comments you make on YouTube videos.

Information we collect as you use our services

Your apps, browsers & devices

We collect information about the apps, browsers, and devices you use to access Google services, which helps us provide features like automatic product updates and dimming your screen if your battery runs low.

The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request.

We collect this information when a Google service on your device contacts our servers — for example, when you install an app from the Play Store or when a service checks for automatic updates. If you're using an Android device with Google apps, your device periodically contacts Google servers to provide information about your device and connection to our services. This information includes things like your device type and carrier name, crash reports, which apps you've installed, and, depending on your device settings, other information about how you're using your Android device.

Your activity

We collect information about your activity in our services, which we use to do things like recommend a YouTube video you might like. The activity information we collect may include:

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

If you use our services to make and receive calls or send and receive messages, we may collect call and message log information like your phone number, calling-party number, receiving-party number, forwarding numbers, sender and recipient email address, time and date of calls and messages, duration of calls, routing information, and types and volumes of calls and messages.

You can visit your Google Account to find and manage activity information that's saved in your account.



[Go to Google Account](#)

Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions, search results for things near you, and ads based on your general location.

Your location can be determined with varying degrees of accuracy by:

- GPS and other sensor data from your device
- IP address
- Activity on Google services, such as your searches and places you label like home or work
- Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

The types of location data we collect and how long we store it depend in part on your device and account settings. For example, you can [turn your Android device's location on or off](#) using the device's settings app. You can also turn on [Location History](#) if you want to create a private map of where you go with your signed-in devices. And if your Web & App Activity setting is enabled, your searches and other activity from Google services, which may also include location information, is saved to your Google Account. Learn more about [how we use location information](#).

In some circumstances, Google also collects information about you from publicly accessible sources. For example, if your name appears in your local newspaper, Google's Search engine may index that article and display it to other people if they search for your name. We may also collect information about you from trusted partners, such as directory services who provide us with business information to be displayed on

Google's services, marketing partners who provide us with information about potential customers of our business services, and security partners who provide us with information to protect against abuse. We also receive information from advertising partners to provide advertising and research services on their behalf.

We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.

WHY GOOGLE COLLECTS DATA

We use data to build better services

We use the information we collect from all our services for the following purposes:

Provide our services

We use your information to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients from your contacts.

Maintain & improve our services

We also use your information to ensure our services are working as intended, such as tracking outages or troubleshooting issues that you report to us. And we use your information to make improvements to our services – for example, understanding which search terms are most frequently misspelled helps us improve spell-check features used across our services.

Develop new services

We use the information we collect in existing services to help us develop new ones. For example, understanding how people organized their photos in Picasa, Google's first photos app, helped us design and launch Google Photos.

Provide personalized services, including content and ads

We use the information we collect to customize our services for you, including providing recommendations, personalized content, and customized search results. For example, [Security Checkup](#) provides security tips adapted to how you use Google products. And Google Play uses information like apps you've already installed and videos you've watched on YouTube to suggest new apps you might like.

Depending on your settings, we may also show you personalized ads based on your interests. For example, if you search for “mountain bikes,” you may see an ad for sports equipment when you’re browsing a site that shows ads served by Google. You can control what information we use to show you ads by visiting your ad settings in [My Ad Center](#).

- We don’t show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.
- We don’t show you personalized ads based on your content from Drive, Gmail, or Photos.
- We don’t share information that personally identifies you with advertisers, such as your name or email, unless you ask us to. For example, if you see an ad for a nearby flower shop and select the “tap to call” button, we’ll connect your call and may share your phone number with the flower shop.



[Go to My Ad Center](#)

Measure performance

We use data for analytics and measurement to understand how our services are used. For example, we analyze data about your visits to our sites to do things like optimize product design. And we also use data about the ads you interact with to help advertisers understand the performance of their ad campaigns. We use a variety of tools to do this, including Google Analytics. When you visit sites or use apps that use Google Analytics, a Google Analytics customer may choose to enable Google to link information about your activity from that site or app with activity from other sites or apps that use our ad services.

Communicate with you

We use information we collect, like your email address, to interact with you directly. For example, we may send you a notification if we detect suspicious activity, like an attempt to sign in to your Google Account from an unusual location. Or we may let you know about upcoming changes or improvements to our services. And

if you contact Google, we'll keep a record of your request in order to help solve any issues you might be facing.

Protect Google, our users, and the public

We use information to help improve the safety and reliability of our services. This includes detecting, preventing, and responding to fraud, abuse, security risks, and technical issues that could harm Google, our users, or the public.

We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

If other users already have your email address or other information that identifies you, we may show them your publicly visible Google Account information, such as your name and photo. This helps people identify an email coming from you, for example.

We'll ask for your consent before using your information for a purpose that isn't covered in this Privacy Policy.

YOUR PRIVACY CONTROLS

You have choices regarding the information we collect and how it's used

This section describes key controls for managing your privacy across our services. You can also visit the [Privacy Checkup](#), which provides an opportunity to review and adjust important privacy settings. In addition

to these tools, we also offer specific privacy settings in our products — you can learn more in our [Product Privacy Guide](#).



[Go to Privacy Checkup](#)

Managing, reviewing, and updating your information

When you're signed in, you can always review and update information by visiting the services you use. For example, Photos and Drive are both designed to help you manage specific types of content you've saved with Google.

We also built a place for you to review and control information saved in your Google Account. Your [Google Account](#) includes:

Privacy controls



Activity Controls

Decide what types of activity you'd like saved in your account. For example, if you have YouTube History turned on, the videos you watch and the things you search for are saved in your account so you can get better recommendations and remember where you left off. And if you have Web & App Activity turned on, your searches and activity from other Google services are saved in your account so you can get more personalized experiences like faster searches and more helpful app and content recommendations. Web & App Activity also has a subsetting that lets you control whether [information about your activity on other sites, apps, and devices that use Google services](#), such as apps you install and use on Android, is saved in your Google Account and used to improve Google services.

[Go to Activity Controls](#)



Ad settings

Manage your preferences about the ads shown to you on Google and on sites and apps that [partner with Google](#) to show ads. You can modify your interests, choose whether your personal information is used to make ads more relevant to you, and turn on or off certain advertising services.

[Go to My Ad Center](#)



About you

Manage personal info in your Google Account and control who can see it across Google services.

[Go to About You](#)



Shared endorsements

Choose whether your name and photo appear next to your activity, like reviews and recommendations, that appear in ads.

[Go to Shared Endorsements](#)



Sites and apps that use Google services

Manage information that websites and apps using Google services, like Google Analytics, may share with Google when you visit or interact with their services.

[Go to How Google uses information from sites or apps that use our services](#)

Ways to review & update your information



My Activity

My Activity allows you to review and control data that's saved to your Google Account when you're signed in and using Google services, like searches you've done or your visits to Google Play. You can browse by date and by topic, and delete part or all of your activity.

[Go to My Activity](#)



Google Dashboard

Google Dashboard allows you to manage information associated with specific products.

[Go to Dashboard](#)



Your personal information

Manage your contact information, such as your name, email, and phone number.

[Go to Personal Info](#)

When you're signed out, you can manage information associated with your browser or device, including:

- Signed-out search personalization: [Choose](#) whether your search activity is used to offer you more relevant results and recommendations.
- YouTube settings: Pause and delete your [YouTube Search History](#) and your [YouTube Watch History](#).
- Ad Settings: [Manage](#) your preferences about the ads shown to you on Google and on sites and apps that partner with Google to show ads.

Exporting, removing & deleting your information

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.



[Export your data](#)

To delete your information, you can:

- Delete your content from [specific Google services](#)
- Search for and then delete specific items from your account using [My Activity](#)
- [Delete specific Google products](#), including your information associated with those products
- [Delete your entire Google Account](#)



[Delete your information](#)

[Inactive Account Manager](#) allows you to give someone else access to parts of your Google Account in case you're unexpectedly unable to use your account.

And finally, you can also [request to remove content](#) from specific Google services based on applicable law and our policies.

There are other ways to control the information Google collects whether or not you're signed in to a Google Account, including:

- Browser settings: For example, you can configure your browser to indicate when Google has set a [cookie](#) in your browser. You can also configure your browser to block all cookies from a specific domain or all domains. But remember that our services [rely on cookies to function properly](#), for things like remembering your language preferences.
 - Device-level settings: Your device may have controls that determine what information we collect. For example, you can [modify location settings](#) on your Android device.
-

SHARING YOUR INFORMATION

When you share your information

Many of our services let you share information with other people, and you have control over how you share. For example, you can share videos on YouTube publicly or you can decide to keep your videos private. Remember, when you share information publicly, your content may become accessible through search engines, including Google Search.

When you're signed in and interact with some Google services, like leaving comments on a YouTube video or reviewing an app in Play, your name and photo appear next to your activity. We may also display this information in [ads depending on your Shared endorsements setting](#).

When Google shares your information

We do not share your personal information with companies, organizations, or individuals outside of Google except in the following cases:

With your consent

We'll share personal information outside of Google when we have your consent. For example, if you [use Google Home to make a reservation](#) through a booking service, we'll get your permission before sharing your name or phone number with the restaurant. We also provide you with controls to [review and manage third party apps and sites](#) you have given access to data in your Google Account. We'll ask for your explicit consent to share any [sensitive personal information](#).

With domain administrators

If you're a student or work for an organization that uses Google services, your [domain administrator](#) and resellers who manage your account will have access to your Google Account. They may be able to:

- Access and retain information stored in your account, like your email
- View statistics regarding your account, like how many apps you install
- Change your account password
- Suspend or terminate your account access
- Receive your account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request
- Restrict your ability to delete or edit your information or your privacy settings

For external processing

We provide personal information to our [affiliates](#) and other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures. For example, we use service providers to help operate our data centers, deliver our products and services, improve our internal business processes, and offer additional support to customers and users. We also use service providers to help review YouTube video content for public safety and analyze and listen to samples of saved user audio to help improve Google's audio recognition technologies.

For legal reasons

We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to:

- Meet any applicable law, regulation, legal process, or enforceable governmental request. We share information about the number and type of requests we receive from governments in our [Transparency Report](#).
- Enforce applicable Terms of Service, including investigation of potential violations.
- Detect, prevent, or otherwise address fraud, security, or technical issues.
- Protect against harm to the rights, property or safety of Google, our users, or the public as required or permitted by law.

We may share non-personally identifiable information publicly and with our partners – like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

If Google is involved in a merger, acquisition, or sale of assets, we'll continue to ensure the confidentiality of your personal information and give affected users notice before personal information is transferred or becomes subject to a different privacy policy.

KEEPING YOUR INFORMATION SECURE

We build security into our services to protect your information

All Google products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. And if we do detect something risky that we think you should know about, we'll notify you and help guide you through steps to stay better protected.

We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information we hold, including:

- We use encryption to keep your data private while in transit

- We offer a range of security features, like [Safe Browsing](#), Security Checkup, and [2 Step Verification](#) to help you protect your account
 - We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
 - We restrict access to personal information to Google employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations.
-

EXPORTING & DELETING YOUR INFORMATION

You can export a copy of your information or delete it from your Google Account at any time

You can export a copy of content in your Google Account if you want to back it up or use it with a service outside of Google.



[Export your data](#)

To delete your information, you can:

- Delete your content from [specific Google services](#)
 - Search for and then delete specific items from your account using [My Activity](#)
 - [Delete specific Google products](#), including your information associated with those products
 - [Delete your entire Google Account](#)
-



[Delete your information](#)

RETAINING YOUR INFORMATION

We retain the data we collect for different periods of time depending on what it is, how we use it, and how you configure your settings:

- Some data you can delete whenever you like, such as your [personal info](#) or the content you create or upload, like [photos](#) and [documents](#). You can also delete [activity information](#) saved in your account, or [choose to have it deleted automatically](#) after a set period of time. We'll keep this data in your Google Account until you remove it or choose to have it removed.
- Other data is deleted or anonymized automatically after a set period of time, such as [advertising data](#) in server logs.
- We keep some data until you delete your Google Account, such as information about how often you use our services.
- And some data we retain for longer periods of time when necessary for legitimate business or legal purposes, such as security, fraud and abuse prevention, or financial record-keeping.

When you delete data, we follow a deletion process to make sure that your data is safely and completely removed from our servers or retained only in anonymized form. We try to ensure that our services protect information from accidental or malicious deletion. Because of this, there may be delays between when you delete something and when copies are deleted from our active and backup systems.

You can read more about Google's [data retention periods](#), including how long it takes us to delete your information.

COMPLIANCE & COOPERATION WITH REGULATORS

We regularly review this Privacy Policy and make sure that we process your information in ways that comply with it.

Data transfers

We maintain [servers around the world](#) and your information may be processed on servers located outside of the country where you live. Data protection laws vary among countries, with some providing more protection than others. Regardless of where your information is processed, we apply the same protections described in this policy. We also comply with certain [legal frameworks](#) relating to the transfer of data.

When we receive formal written complaints, we respond by contacting the person who made the complaint. We work with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of your data that we cannot resolve with you directly.

U.S. state law requirements

Some U.S. state privacy laws like the California Consumer Privacy Act (CCPA) and Virginia Consumer Data Protection Act (VCDPA) require specific disclosures for state residents.

This Privacy Policy is designed to help you understand how Google handles your information:

- We explain the categories of information Google collects and the sources of that information in [Information Google collects](#).
- We explain how Google uses information in [Why Google collects data](#).
- We explain when Google may disclose information in [Sharing your information](#). Google does not sell your personal information. Google also does not “share” your personal information as that term is defined in the CCPA.
- We explain how Google retains information in [Retaining your information](#). You can also learn more about [how Google anonymizes data](#). As described there, when Google anonymizes data to protect your privacy, we maintain policies and technical measures to avoid re-identifying that information.

State laws like the CCPA and VCDPA also provide the right to request information about how Google collects, uses, and discloses your information. And they give you the right to access and correct your information, and to request that Google delete that information. The VCDPA also provides the right to opt out of certain forms of profiling and targeted advertising. Finally, the CCPA and VCDPA provide the right to not be discriminated against for exercising these privacy rights.

We describe the choices you have to manage your privacy and data across Google’s services in [Your privacy controls](#). These tools allow you to access, review, update and delete your information, as well as [export and download](#) a copy of it. You can also control what information we use to show you ads, or turn off personalized ads, by visiting [My Ad Center](#).

When you use these tools, we’ll validate your request by verifying that you’re signed in to your Google Account. If you have questions or requests related to your rights under the CCPA or VCDPA, you (or your authorized agent) can also [contact Google](#). And if you disagree with the decision on your request, you can ask Google to reconsider it by responding to the team’s email.

You can find [more information](#) on Google's handling of CCPA requests.

The CCPA also requires a description of data practices using specific categories. This table uses these categories to organize the information in this Privacy Policy.

Categories of information we collect

Identifiers and similar information such as your [name](#) and password, phone number, and address, as well as unique identifiers tied to the browser, application, or device you're using. Some Google services like [YouTube Studio](#) provide the option to submit a valid ID (such as a passport or driver's license) to verify your identity to use additional features.

Demographic information, such as your [age](#), [gender](#) and [language](#). If you choose to use optional features like [YouTube Creator Demographics](#), you can also provide additional information, like your gender identity or race and ethnicity.

Commercial information such as your [payment information](#) and a history of [purchases](#) you make on Google's services.

Biometric information if you choose to provide it, such as fingerprints in Google's product development studies.

Internet, network, and other activity information such as your search terms; views and interactions with content and ads; Chrome browsing history you've synced with your Google Account; information about the interaction of your apps, browsers, and devices with our services (like IP address, crash reports, and system activity); and activity on third-party sites and apps that use our services. You can review and control activity data stored in your Google Account in [My Activity](#).

Geolocation data, such as may be determined by GPS, IP address, and other data from sensors on or around your device, depending in part on your device and account settings. Depending on these settings, this may include **precise location data**, for example GPS data for Android features like navigation or finding your phone. Learn more about [Google's use of location information](#).

Audio, electronic, visual, and similar information, such as voice and audio information.

Communications data, such as emails, if you use our services to send and receive messages.

Health information if you choose to provide it, such as your medical history, vital signs and health metrics (like blood glucose levels), and other similar information related to your physical or mental health, in the course of using Google services that offer health-related features, such as the [Google Health Studies app](#).

Professional, employment, and education information, such as information [you provide](#) or that is maintained through an organization using Google services at which you study or work.

Other information you create or provide, such as the content you create, upload, or receive (like photos and videos or emails, docs and spreadsheets). [Google Dashboard](#) allows you to manage information associated with specific products.

Inferences drawn from the above, like your [ads interest categories](#).

Business purposes for which information may be used or disclosed

Protecting against security threats, abuse, and illegal activity: Google uses and may disclose information to detect, prevent and respond to security incidents, and for protecting against other malicious, deceptive, fraudulent, or illegal activity. For example, to protect our services, Google may receive or disclose information about IP addresses that malicious actors have compromised.

Auditing and measurement: Google uses information for analytics and measurement to understand how our services are used, as well as to fulfill obligations to our partners like publishers, advertisers, developers, or rights holders. We may disclose non-personally identifiable information publicly and with these partners, including for auditing purposes.

Maintaining our services: Google uses information to ensure our services are working as intended, such as tracking outages or troubleshooting bugs and other issues that you report to us.

Research and development: Google uses information to improve our services and to develop new products, features and technologies that benefit our users and the public. For example, we use publicly available information to help train Google's language models and build features like Google Translate.

Use of service providers: Google shares information with service providers to perform services on our behalf, in compliance with our Privacy Policy and other appropriate confidentiality and security measures. For example, we may rely on service providers to help provide customer support.

Advertising: Google processes information to provide advertising, including online identifiers, browsing and search activity, and information about your location and interactions with advertisements. This keeps

Google's services and many of the websites and services you use free of charge. You can control what information we use to show you ads by visiting your ad settings in [My Ad Center](#).

Legal reasons: Google also uses information to satisfy applicable laws or regulations, and discloses information in response to legal process or enforceable government requests, including to law enforcement. We provide information about the number and type of requests we receive from governments in our [Transparency Report](#).

Parties with whom information may be disclosed

Other people with whom you choose to share your information, like docs or photos, and videos or comments on YouTube.

Third parties with your consent, such as services that integrate with Google's services. You can [review and manage third party apps and sites](#) with access to data in your Google Account.

Service providers, trusted businesses or persons that process information on Google's behalf, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.

Domain administrators, if you work or study at an organization that uses Google services.

Law enforcement or other third parties, for the legal reasons described in [Sharing your information](#).

ABOUT THIS POLICY

When this policy applies

This Privacy Policy applies to all of the services offered by Google LLC and its affiliates, including YouTube, Android, and services offered on third-party sites, such as advertising services. This Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy.

This Privacy Policy doesn't apply to:

- The information practices of other companies and organizations that advertise our services

- Services offered by other companies or individuals, including products or sites they offer that may include Google services to which the policy applies, or products or sites displayed to you in search results, or linked from our services

Changes to this policy

We change this Privacy Policy from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent. We always indicate the date the last changes were published and we offer access to [archived versions](#) for your review. If changes are significant, we'll provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes).

RELATED PRIVACY PRACTICES

Specific Google services

The following privacy notices provide additional information about some Google services:

- [Chrome & the Chrome Operating System](#)
- [Payments](#)
- [Fiber](#)
- [Google Fi](#)
- [Google Workspace for Education](#)
- [Read Along](#)
- [YouTube Kids](#)
- [Google Accounts Managed with Family Link, for Children under 13 \(or applicable age in your country\)](#)
- [Family Link privacy guide for children & teens](#)
- [Voice and Audio Collection from Children's Features on the Google Assistant](#)

If you're a member of an organization that uses Google Workspace or Google Cloud Platform, learn how these services collect and use your personal information in the [Google Cloud Privacy Notice](#).

Other useful resources

The following links highlight useful resources for you to learn more about our practices and privacy settings.

- [Your Google Account](#) is home to many of the settings you can use to manage your account
- [Privacy Checkup](#) guides you through key privacy settings for your Google Account
- [Google's safety center](#) helps you learn more about our built-in security, privacy controls, and tools to help set digital ground rules for your family online
- [Google's Teen Privacy Guide](#) provides answers to some of the top questions we get asked about privacy
- [Privacy & Terms](#) provides more context regarding this Privacy Policy and our Terms of Service
- [Technologies](#) includes more information about:
 - [How Google uses cookies](#)
 - [Technologies used for Advertising](#)
 - [How Google uses information from sites or apps that use our services](#)

Key terms

Affiliates

An affiliate is an entity that belongs to the Google group of companies, including the following companies that provide consumer services in the EU: Google Ireland Limited, Google Commerce Ltd, Google Payment Corp, and Google Dialer Inc. Learn more about the [companies providing business services in the EU](#).

Algorithm

A process or set of rules followed by a computer in performing problem-solving operations.

Application data cache

An application data cache is a data repository on a device. It can, for example, enable a web application to run without an internet connection and improve the performance of the application by enabling faster loading of content.

Browser web storage

Browser web storage enables websites to store data in a browser on a device. When used in "local storage" mode, it enables data to be stored across sessions. This makes data retrievable even after a browser has been closed and reopened. One technology that facilitates web storage is HTML 5.

Cookies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the site again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

Device

A device is a computer that can be used to access Google services. For example, desktop computers, tablets, smart speakers, and smartphones are all considered devices.

Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address, and a password). This account information is used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

IP address

Every device connected to the Internet is assigned a number known as an Internet protocol (IP) address. These numbers are usually assigned in geographic blocks. An IP address can often be used to identify the location from which a device is connecting to the Internet.

Non-personally identifiable information

This is information that is recorded about users so that it no longer reflects or references an individually-identifiable user.

Personal information

This is information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account.

Pixel tag

A pixel tag is a type of technology placed on a website or within the body of an email for the purpose of tracking certain activity, such as views of a website or when an email is opened. Pixel tags are often used in combination with cookies.

Referrer URL

A Referrer URL (Uniform Resource Locator) is information transmitted to a destination webpage by a web browser, typically when you click a link to that page. The Referrer URL contains the URL of the last webpage the browser visited.

Sensitive personal information

This is a particular category of personal information relating to topics such as confidential medical facts, racial or ethnic origins, political or religious beliefs, or sexuality.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These “server logs” typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser.

A typical log entry for a search for “cars” looks like this:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
http://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 -
740674ce2123e969
```

- `123.45.67.89` is the Internet Protocol address assigned to the user by the user’s ISP. Depending on the user’s service, a different address may be assigned to the user by their service provider each time they connect to the Internet.
- `25/Mar/2003 10:15:32` is the date and time of the query.
- `http://www.google.com/search?q=cars` is the requested URL, including the search query.
- `Firefox 1.0.7; Windows NT 5.1` is the browser and operating system being used.
- `740674ce2123a969` is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time they’ve visited Google, then it will be the unique cookie ID assigned to their device the next time they visit Google from that particular device).

Unique identifiers

A unique identifier is a string of characters that can be used to uniquely identify a browser, app, or device. Different identifiers vary in how permanent they are, whether they can be reset by users, and how they can be accessed.

Unique identifiers can be used for various purposes, including security and fraud detection, syncing services such as your email inbox, remembering your preferences, and providing personalized advertising. For example, unique identifiers stored in cookies help sites display content in your browser in your preferred language. You can configure your browser to refuse all cookies or to indicate when a cookie is being sent. Learn more about [how Google uses cookies](#).

On other platforms besides browsers, unique identifiers are used to recognize a specific device or app on that device. For example, a unique identifier such as the Advertising ID is used to provide relevant advertising on Android devices, and can be [managed](#) in your device's settings. Unique identifiers may also be incorporated into a device by its manufacturer (sometimes called a universally unique ID or UUID), such as the IMEI-number of a mobile phone. For example, a device's unique identifier can be used to customize our service to your device or analyze device issues related to our services.

Additional Context

ads you'll find most useful

For example, if you watch videos about baking on YouTube, you may see more ads that relate to baking as you browse the web. We also may use your IP address to determine your approximate location, so that we can serve you ads for a nearby pizza delivery service if you search for "pizza." Learn more [about Google ads](#) and [why you may see particular ads](#).

advertising and research services on their behalf

For example, advertisers may upload data from their loyalty-card programs so that they can better understand the performance of their ad campaigns. We only provide aggregated reports to advertisers that don't reveal information about individual people.

Android device with Google apps

Android devices with Google apps include devices sold by Google or one of our partners and include phones, cameras, vehicles, wearables, and televisions. These devices use Google Play Services and other pre-installed apps that include services like Gmail, Maps, your phone's camera and phone dialer, text-to-speech conversion, keyboard input, and security features. Learn more [about Google Play Services](#).

combine the information we collect

Some examples of how we combine the information we collect include:

- When you're signed in to your Google Account and search on Google, you can see search results from the public web, along with relevant information from the content you have in other Google products, like

Gmail or Google Calendar. This can include things like the status of your upcoming flights, restaurant, and hotel reservations, or your photos. [Learn more](#)

- If you have communicated with someone via Gmail and want to add them to a Google Doc or an event in Google Calendar, Google makes it easy to do so by autocompleting their email address when you start to type in their name. This feature makes it easier to share things with people you know. [Learn more](#)
- The Google app can use data that you have stored in other Google products to show you personalized content, depending on your settings. For example, if you have searches stored in your Web & App Activity, the Google app can show you news articles and other information about your interests, like sports scores, based on your activity. [Learn more](#)
- If you link your Google Account to your Google Home, you can manage your information and get things done through the Google Assistant. For example, you can add events to your Google Calendar or get your schedule for the day, ask for status updates on your upcoming flight, or send information like driving directions to your phone. [Learn more](#)

customized search results

For example, when you're signed in to your Google Account and have the Web & App Activity control enabled, you can get more relevant search results that are based on your previous searches and activity from other Google services. You can [learn more here](#). You may also get customized search results even when you're signed out. If you don't want this level of search customization, you can [search and browse privately](#) or turn off [signed-out search personalization](#).

deliver our services

Examples of how we use your information to deliver our services include:

- We use the IP address assigned to your device to send you the data you requested, such as loading a YouTube video
- We use unique identifiers stored in cookies on your device to help us authenticate you as the person who should have access to your Google Account
- Photos and videos you upload to Google Photos are used to help you create albums, animations, and other creations that you can share. [Learn more](#)
- A flight confirmation email you receive may be used to create a "check-in" button that appears in your Gmail

- When you purchase services or physical goods from us, you may provide us information like your shipping address or delivery instructions. We use this information for things like processing, fulfilling, and delivering your order, and to provide support in connection with the product or service you purchase.

detect abuse

When we detect spam, malware, illegal content, and other forms of abuse on our systems in violation of our policies, we may disable your account or take other appropriate action. In certain circumstances, we may also report the violation to appropriate authorities.

devices

For example, we can use information from your devices to help you decide which device you'd like to use to install an app or view a movie you buy from Google Play. We also use this information to help protect your account.

ensure and improve

For example, we analyze how people interact with advertising to improve the performance of our ads.

ensure our services are working as intended

For example, we continuously monitor our systems to look for problems. And if we find something wrong with a specific feature, reviewing activity information collected before the problem started allows us to fix things more quickly.

Information about things near your device

If you use Google's Location services on Android, we can improve the performance of apps that rely on your location, like Google Maps. If you use Google's Location services, your device sends information to Google about its location, sensors (like accelerometer), and nearby cell towers and Wi-Fi access points (like MAC address and signal strength). All these things help to determine your location. You can use your device settings to enable Google Location services. [Learn more](#)

legal process, or enforceable governmental request

Like other technology and communications companies, Google regularly receives requests from governments and courts around the world to disclose user data. Respect for the privacy and security of data you store with Google underpins our approach to complying with these legal requests. Our legal team reviews each and every request, regardless of type, and we frequently push back when a request appears to be overly broad or doesn't follow the correct process. Learn more in our [Transparency Report](#).

make improvements

For example, we use cookies to analyze how people interact with our services. And that analysis can help us build better products. For example, it may help us discover that it's taking people too long to complete a certain task or that they have trouble finishing steps at all. We can then redesign that feature and improve the product for everyone.

may link information

Google Analytics relies on first-party cookies, which means the cookies are set by the Google Analytics customer. Using our systems, data generated through Google Analytics can be linked by the Google Analytics customer and by Google to third-party cookies that are related to visits to other websites. For example, an advertiser may want to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. [Learn more](#)

our users

For example, to prevent abuse and increase transparency and accountability over our online content moderation practices, Google shares data about requests for removal of content from our services with Lumen, which collects and analyzes these requests to facilitate research to help Internet users understand their rights. [Learn more](#).

partner with Google

There are over 2 million non-Google websites and apps that partner with Google to show ads. [Learn more](#)

payment information

For example, if you add a credit card or other payment method to your Google Account, you can use it to buy things across our services, like apps in the Play Store. We may also ask for other information, like a business tax ID, to help process your payment. In some cases, we may also need to verify your identity and may ask you for information to do this.

We may also use payment information to verify that you meet age requirements, if, for example, you enter an incorrect birthday indicating you're not old enough to have a Google Account. [Learn more](#)

personalized ads

You may also see personalized ads based on information from the advertiser. If you shopped on an advertiser's website, for example, they can use that visit information to show you ads. [Learn more](#)

phone number

If you add your phone number to your account, it can be used for different purposes across Google services, depending on your settings. For example, your phone number can be used to help you access your account if you forget your password, help people find and connect with you, and make the ads you see more relevant to you. [Learn more](#)

protect against abuse

For example, information about security threats can help us notify you if we think your account has been compromised (at which point we can help you take steps to protect your account).

publicly accessible sources

For example, we may collect information that's publicly available online or from other public sources to help train Google's language models and build features like Google Translate. Or, if your business's information appears on a website, we may index and display it on Google services.

rely on cookies to function properly

For example, we use a cookie called 'lbc' that makes it possible for you to open many Google Docs in one browser. Blocking this cookie would prevent Google Docs from working as expected. [Learn more](#)

safety and reliability

Some examples of how we use your information to help keep our services safe and reliable include:

- Collecting and analyzing IP addresses and cookie data to protect against automated abuse. This abuse takes many forms, such as sending spam to Gmail users, stealing money from advertisers by fraudulently clicking on ads, or censoring content by launching a Distributed Denial of Service (DDoS) attack.
- The "last account activity" feature in Gmail can help you find out if and when someone accessed your email without your knowledge. This feature shows you information about recent activity in Gmail, such as the IP addresses that accessed your mail, the associated location, and the date and time of access.
[Learn more](#)

sensitive categories

When showing you personalized ads, we use topics that we think might be of interest to you based on your activity. For example, you may see ads for things like "Cooking and Recipes" or "Air Travel." We don't use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we [require the same from advertisers](#) that use our services.

Sensor data from your device

Your device may have sensors that can be used to better understand your location and movement. For example, an accelerometer can be used to determine your speed and a gyroscope to figure out your direction of travel.

servers around the world

For example, we operate data centers located [around the world](#) to help keep our products continuously available for users.

services to make and receive calls or send and receive messages

Examples of these services include:

- Google Voice, for making and receiving calls, sending text messages, and managing voicemail
- Google Meet, for making and receiving video calls
- Gmail, for sending and receiving emails
- Google Chat, for sending and receiving messages
- Google Duo, for making and receiving video calls and sending and receiving messages
- Google Fi, for a phone plan

show trends

When lots of people start searching for something, it can provide useful information about particular trends at that time. Google Trends samples Google web searches to estimate the popularity of searches over a certain period of time and shares those results publicly in aggregated terms. [Learn more](#)

specific Google services

For example, you can delete [your blog](#) from Blogger or [a Google Site you own](#) from Google Sites. You can also delete [reviews](#) you've left on apps, games, and other content in the Play Store.

specific partners

For example, we allow YouTube creators and advertisers to work with measurement companies to learn about the audience of their YouTube videos or ads, using cookies or similar technologies. Another example is merchants on our shopping pages, who use cookies to understand how many different people see their product listings. [Learn more](#) about these partners and how they use your information.

synced with your Google Account

Your Chrome browsing history is only saved to your account if you've enabled Chrome synchronization with your Google Account. [Learn more](#)

the people who matter most to you online

For example, when you type an address in the To, Cc, or Bcc field of an email you're composing, Gmail will suggest addresses based on the people you [contact most frequently](#).

the public

For example, we process information about [requests to remove content](#) from our services under Google's content removal policies or applicable law to assess the request, and to ensure transparency, improve accountability and prevent abuse and fraud in these practices.

third parties

For example, we process your information to report use statistics to rights holders about how their content was used in our services. We may also process your information if people search for your name and we display search results for sites containing publicly available information about you.

Views and interactions with content and ads

For example, we collect information about views and interactions with ads so we can provide aggregated reports to advertisers, like telling them whether we served their ad on a page and whether the ad was likely seen by a viewer. We may also measure other interactions, such as how you move your mouse over an ad or if you interact with the page on which the ad appears.

Voice and audio information

For example, you can choose whether you want Google to save an audio recording to your Google Account when you interact with Google Search, Assistant, and Maps. When your device detects an audio activation

command, like "Hey Google," Google records your voice and audio plus a few seconds before the activation.

[Learn more](#)

your activity on other sites and apps

This activity might come from your use of Google services, like from syncing your account with Chrome or your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your [account settings](#) and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.

[Learn more](#) about how Google uses data when you use our partners' sites or apps.

EXHIBIT 113

**9/1/15
CHROME
PRIVACY
NOTICE**

Google Chrome Privacy Notice

Archive date: September 1, 2015

Chromecast is covered by the [Google Privacy Policy](#). [Learn more.](#)

The [Google Privacy Policy](#) describes how we treat personal information when you use Google's products and services, including when you use Chrome browser and Chrome OS to access those products and services.

This Google Chrome Privacy Notice describes the privacy practices that are specific to the Chrome family of products. This includes the Chrome browser, Chrome OS, and Safe Browsing. Some of the features described in this Privacy Notice are available in other web browsers (e.g. you may choose to use Safe Browsing features in Mozilla Firefox), so remember that you should also read the privacy policy for the browser in which the features are running.

Not all of the features discussed in this Privacy Notice appear in all Chrome products. To keep things simple, however, we're going to use the term "Chrome" on its own to refer to each of the products within the Chrome family. Where an individual Chrome product works in a different way we'll be sure to highlight that.

For early adopters who want to test features that are still under development, we make available preview versions (also known as beta, dev and canary) of Chrome browser and Chrome OS in addition to the stable version. Although this Google Chrome Privacy Notice applies to the stable and preview versions, it may not be fully up to date when describing features still under development in the [preview versions](#).

Google will notify you of any material changes to this policy, and you will always have the option to use Chrome in a way that does not send any personally identifiable information to Google, or to remove your information and discontinue using it.

For step-by-step guides to help manage your privacy preferences read our guide to [Browsers](#), [Google Chrome](#), [Privacy and You](#).

Information Google receives when you use Chrome

You do not need to provide any personally identifying information in order to use Chrome.

When you use any browser, including Chrome, to contact Google's servers, by default Google receives standard log information including your system's IP address and one or more cookies. You can configure Chrome browser and Chrome OS to not accept cookies from Google or other sites. Learn more about configuring cookies and site data in Chrome browser and Chrome OS.

If you use Chrome to access other Google services, such as using the search engine on the Google homepage or checking Gmail, the fact that you are using Chrome does not cause Google to receive any special or additional personally identifying information about you.

In addition, some Chrome features may send limited additional information to Google or your default search engine.

- If you use the Multiple Users feature of Chrome browser, you can set up personalized copies of Chrome browser for users who are sharing the same computing device. It isn't intended to secure your data against other people using your device - so anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system.
- If you choose Google as your search engine, Chrome will contact Google when it starts or when you change networks so as to determine the best local web address to send search queries. When you type URLs or queries in the Chrome address bar (omnibox) or App Launcher search box, the letters you type may be sent to your default search engine so that the search engine's prediction feature can automatically recommend terms or URLs you may be looking for. Additionally, for signed in users, the text that you type into the App Launcher search box can be sent to Google to provide recommendations for the contacts and the apps you might be looking for. If you accept a predicted query or URL, Chrome may send that information from the browser to your default search engine as well. Learn more about disabling server predictions in the omnibox and Google's logging policies for omnibox predictions.
- On mobile versions of the Chrome browser, you can enable "Touch to Search" which allows you to tap on a word to see a suggested search term. The word you tapped, the content of the page, and the URL of the page you're on will be sent to Google to provide the recommended search term.

- If you enable the feature in your device's Today view, you can use Chrome on your iPhone or iPad to discover objects around you that are broadcasting web addresses as part of the Physical Web. When you use this feature, Chrome sends the web addresses broadcast by these objects to a Google server to find the title of the web page and help rank the results. The information sent to Google to provide this feature does not include any personal information from your device.
- If you navigate to a URL that does not exist, Chrome may send the URL to Google so we can help you find the URL you were looking for. We may also use this information in an aggregated way to help other web users - e.g. to let them know that the site may be down. Learn more about [disabling suggestions on navigation errors](#).
- Chrome periodically contacts Google to perform functions such as checking for updates, checking connectivity status, validating current time, and estimating the number of active users. Each copy of Chrome browser includes a temporary randomly-generated installation number which will be sent to Google when you install and first use the product. The temporary number will be promptly deleted the first time that Chrome browser automatically checks for updates. If you received or reactivated your copy of the Chrome browser as part of a promotional campaign, it may also generate a non-unique promotional tag which is sent to Google when performing searches with Google and a unique token which is sent to Google when you first run and use the browser after installation, reinstallation, or reactivation. Chrome OS may send a non-unique promotional tag to Google periodically (including during initial set up) and when performing searches with Google. Furthermore, [field trials](#) may result in different variations of Chrome, and Chrome may send non-unique information to Google about which variation is active.
- If you grant an application, extension, or website permission to use Google's Cloud Messaging, or if you use Chrome Sync, Chrome generates a randomly chosen device ID. This device ID is shared with Google but not accessible to third parties, and is revoked once it is no longer in use or when the Chrome profile is removed. From the device ID, Chrome then derives a registration ID that is shared with applications, extensions, or websites to securely pass messages from Google's servers to the browser.
- Chrome OS contacts Google during initial device setup to determine if the device is subject to policies of an enterprise administrator. This process involves sending Google a part of a hash of a short-lived device identifier and receiving back from Google a list of hashed device identifiers that were possible matches, so Chrome OS may determine if the device is on that list.

- Chrome contacts Google for session policies when a user first signs in to Chrome or starts browsing without signing in (excluding Guest mode) on devices subject to policies. Chrome will check periodically for updates to policies. Enterprise policies may involve status and activity reporting for Chrome (including location information for Chrome OS devices) set up by the enterprise admin.
- If you sign in to Chrome browser, Chrome OS or an Android device that includes Chrome as a preinstalled application with your Google Account, this will enable the synchronization feature. Google will store certain information, such as history, bookmarked URLs as well as an image and a sample of text from the bookmarked page, passwords and other settings, on Google's servers in association with your Google Account. Information stored with your Account is protected by the Google Privacy Policy. We also store this information to make it available to you on other instances of Chrome in which you choose to sign in. Learn more about the specific information you may select to synchronize, and more about disabling Chrome's synchronization feature in Chrome browser.
- If you are signed into Chrome with your Google Account, Google Drive and Docs, Sheets, Slides and Drawings will be automatically enabled for offline use. In that case, or if you otherwise enable offline use of a Google application in Chrome browser or install a Chrome application that stores data in your Google Drive account, Chrome may contact Google's servers and synchronize your data with a local copy to enable offline functionality.
- If you create a supervised user in Chrome browser or on Chrome OS with your Google Account, Google will synchronize and store certain information, such as the supervised user's history and other settings on Google's servers in association with your Google Account. We store this information in order to make it available to you at chrome.com/manage. Information stored with your account is protected by the Google Privacy Policy.
- If you use the Translate feature of Chrome, it will send the text you choose to be translated to Google for translation.
- If you use the Spellcheck feature of Chrome, which lets you use the same technology used in Google search to check your spelling, it will send the text you type to Google for spelling and grammar suggestions.
- If you use the speech input feature of Chrome, it will send Google an audio recording of your spoken query, your default browser language and the grammar settings of the web page for which you are using

speech input. Google will use this information to convert the recorded audio into text. If you have enabled usage statistics and crash reports and you use the speech input feature, additional information will be sent to Google, including the URL of the website using speech input, your operating system, and the manufacturer and model of the computing device and audio hardware you are using.

- If you use Chrome's AutoFill feature, which automatically completes web forms for you based on similar forms you have filled out before, Chrome will send Google limited information about the pages that have web forms, including a hashed URL of the web page and details of the form's structure, so that we can improve our AutoFill service for this web form. While the information that Chrome sends may include the fact that you typed information into the form, the actual text that you type in the fields will not be sent to Google unless you choose to store that data in [your Google Account](#) using Chrome's synchronization feature.
- Some web forms handled by Chrome will offer you the option to use Google Payments rather than Chrome's AutoFill feature to complete the form and make payments. If you use Google Payments, then to protect you from fraud, Chrome will collect information about your computer (including its location) and share it with Google Payments.
- If you use Chrome's location feature, which allows you to share your location with a web site, Chrome will send local network information to Google Location Services to get an estimated location. Learn more about [Google Location Services and enabling / disabling location features within Google Chrome](#). The local network information may include (depending on the capabilities of your device) information about the wifi routers closest to you, cell IDs of the cell towers closest to you, the strength of your wifi or cell signal, and the IP address that is currently assigned to your device. We use the information to process the location request and to operate, support, and improve the overall quality of Chrome and Google Location Services. The collected information described above will be anonymized and aggregated before being used by Google to develop new features or products and services, or to improve the overall quality of any of Google's other products and services.
- If you are using a mobile version of Chrome, and you have granted your Android device or Chrome on iOS permission to access your location, then Chrome may use your location for Google location-enabled services, including for example enhancing omnibox searches.
- If you attempt to connect to a Google website using a secure connection, and the browser blocks the connection due to information that indicates you are being actively attacked by someone on the network

(a "man in the middle attack"), Chrome may send information about that connection to Google for the purpose of helping to determine the extent of the attack and how the attack functions.

- If you enable Chrome's "Reduce data usage" feature on your mobile device, Chrome will send your HTTP traffic through Google's optimizing servers to reduce the amount of data downloaded and improve performance. The optimizing service is disabled for connections to HTTPS origins, and for connections made from Incognito tabs.
- For Chrome browser and Chrome OS, you may choose to send usage statistics and crash reports to Google. You can manage this setting within the Chrome preferences page; for Chrome OS users, usage statistics and crash reports are enabled by default. This setting will apply to all users for a given installation of Chrome. The usage statistics and crash reports help us diagnose problems, help us understand how users interact with Chrome, and help us improve Chrome's performance.
- Chrome tries to avoid sending information that identifies you personally. Crash reports, however, can contain system information at the time of a malfunction, and errors leading up to a malfunction. We may share with third parties certain aggregated, non-personal information we derive from our analysis, such as how frequently certain types of crashes occur.

Information Google receives when you use the Safe Browsing feature on Chrome or other browsers

Google Chrome and certain third party browsers (including some versions of Mozilla's Firefox and Apple's Safari) includes Google's Safe Browsing feature. Safe Browsing sends and receives information between the browser you are using and Google's servers about suspicious websites – for example when you visit a site that is suspected to be a phishing or malware site.

Your browser will contact Google's servers periodically to download the most recent "Safe Browsing" list, containing known phishing and malware sites. Google does not collect any account information or other personally identifying information as part of this contact, but it does receive standard log information, including an IP address and one or more cookies. The most recent copy of the list is stored locally on your system.

Each site you visit will be checked against the Safe Browsing list on your system. If there is a match against the list, your browser will send Google a hashed, partial copy of the site's URL so that Google can send more

Information to your browser. Google cannot determine the real URL from this information. Read more [information about how this works](#).

In addition, the following Safe Browsing features are specific to Chrome:

- Some versions of Chrome feature Safe Browsing technology that can identify potentially harmful sites and executable file downloads not already known by Google. Information regarding a potentially harmful site or executable file download (including the full URL of the site or executable file download) may be sent to Google to help determine whether the site or download is harmful. Google does not collect any account information or other personally identifying information as part of this contact, but does receive [standard log information](#), including an IP address, URL visited and one or more [cookies](#).
- Chrome uses Safe Browsing technology to scan your computer periodically to detect [unwanted software](#) that prevents you from changing your settings or otherwise interferes with the security and stability of your browser. If such software is detected, Chrome may offer you the option to download the [software removal tool](#) to remove it.
- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware. This data is sent when you close or navigate away from a Safe Browsing warning page. The reports contain data, such as the URL and contents of the website as well as the URL of the page that directed you to that site, that can be used by Google to verify whether the site is still serving content that may exploit users.
- If usage statistics are enabled in Chrome and you visit a site that we think could be potentially harmful, certain additional data will be shared with Google, including the full URL that you visited, the "[referer](#)" header sent to that page, and the URL that matched the Safe Browsing list.
- You can always choose to [disable the Safe Browsing feature within Chrome](#).

Information website operators receive when you visit a site using Chrome

Sites that you visit using Chrome will automatically receive [standard log information](#) similar to that received by Google. These sites may also set their own [cookies](#) or store site data on your system. You can restrict [cookies](#) and other site data in Chrome's preferences page.

If Chrome's network actions prediction features are enabled, Chrome may look up the IP addresses of all links on webpages and open network connections to load webpages faster. Sites can also use pre-rendering technology to pre-load the links that you might click next.

If you use Chrome in incognito mode or guest mode, it will not transmit any pre-existing cookies to sites that you visit. Sites may deposit new cookies on your system while you are in these modes; these cookies will only be temporarily stored and transmitted to sites while you remain in incognito / guest mode. They will be deleted when you close the browser, close all open incognito windows or exit guest mode.

If you choose to use Chrome's location feature, this service allows you to share your location with a site. Chrome will not allow a site to access your location without your permission. Google does not have control over third party websites or their privacy practices. Please carefully consider any website's privacy practices before consenting to share your location with that website.

Information stored on your system when you use Chrome

Chrome stores some information locally on your system. This may include:

- Basic browsing history information, for example the URLs of pages that you visit, a cache file of text and images from those pages, and a list of some IP addresses linked from pages that you visit.
- A searchable index of most pages you visit (except for secure pages with "https" web addresses, such as some bank pages)
- Thumbnail-sized screenshots of most pages you visit
- Cookies or web storage data deposited on your system by websites you visit
- Locally-stored data saved by Add-ons
- A record of downloads you have made from websites

You can always choose to delete your browsing history information, in whole or in part.

You can also limit the information Chrome stores on your system by using [incognito mode](#) or guest mode. The Chrome browser offers both modes. Incognito mode is useful if you would still like to have access to information from your existing profile, such as suggestions based on your browsing history, while you are browsing. Guest mode is useful if you would prefer to begin a browsing session without seeing information from any existing profiles. In either of these modes, Chrome will not store basic browsing history information such as URLs, cached page text, or IP addresses of pages linked from the websites you visit. It will also not store snapshots of pages that you visit or keep a record of your downloads (although this information could still be stored elsewhere on your system, e.g. in a list of recently opened files). New [cookies](#) received in these modes will not be saved after you close your browser, close all open incognito windows or exit guest mode. You can see when you are in Incognito / guest mode because the incognito icon appears in the top corner of your browser; in some cases the border of your browser window may also change color.

When you make changes to your browser configuration, such as by bookmarking a web page or changing your settings, this information is also saved. These changes are not affected by Incognito / guest mode.

You can choose to have Chrome save your passwords for specific websites. [Stored passwords can be reviewed](#) in Chrome settings.

Unique Identifiers for Digital Rights Management

In order to allow certain content to be accessed using Chrome browser for Windows or Chrome OS, Chrome may be required to provide selected content partners and websites using Adobe Flash Access with a unique identifier that is stored on your system. You can disable this feature in the settings or reset the unique identifier's value by reinstalling the operating system.

Parties to whom your unique identifier is provided could associate it with personally-identifiable information you provide to them. Google's use of a unique identifier to provide content from Google servers is subject to the Google Privacy Policy. If you are accessing content from a third party service, you should review those parties' privacy policies to learn more.

Using apps, extensions, themes, services, and other add-ons with Chrome

You may use apps, extensions, themes, services and other add-ons ("Add-ons") with Chrome, including some that may be pre-installed or integrated with Chrome and some that you may obtain from [Chrome Web Store](#) or other sources.

Before installing an Add-on, you should review the requested permissions. Add-ons may be designed to store, access, and share data stored locally or in your Google Drive account. Add-ons may use notifications that are sent through Google servers. Chrome may check for, download, and install updates to your Add-ons. Chrome may send usage indicators to Google for installed Add-ons. Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of such an identifier by removing the add-on from Chrome.

From time to time, Google may discover an Add-on that poses a security vulnerability or violates the developer terms for [Chrome Web Store](#) or other legal agreements, laws, regulations or policies. Chrome may periodically download a list of such Add-ons from Google's servers, and Google may remotely disable or remove such Add-ons from user systems in its sole discretion.

Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by third parties are the responsibility of such third parties and may be subject to third party privacy policies. For example, a version of the Adobe Flash Player plug-in is preinstalled with Chrome. Adobe's website at www.adobe.com provides more information on Adobe's privacy practices with regard to Flash Player, and you can learn more about [disabling Flash Player or any other plug-ins](#).

Uses

Information that Google receives when you use Chrome is processed in order to operate and improve Chrome and other Google services. Information that other website operators receive is subject to the privacy policies of those websites. Chrome stores information on your system in order to improve Chrome's performance and to provide you with useful features and services.

More information

Google adheres to the US Safe Harbor privacy principles. For more information about the Safe Harbor framework or our registration, see the [Department of Commerce's web site](#).

Further information about Chrome is [available here](#).

For more information about our privacy practices, go to the [full privacy policy](#). If you have additional questions, [please consult this page](#).

EXHIBIT 114

**6/21/16
CHROME
PRIVACY
NOTICE**

Google Chrome Privacy Notice

Archive date: June 21, 2016

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, Chrome OS, and Safe Browsing. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#).

Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll call it out.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.

For step-by-step guides to managing your privacy preferences, read [this overview of Chrome's privacy controls](#).

Table of contents:

- [Browser modes](#)
- [Managing users in Chrome](#)
- [Safe Browsing policies](#)
- [Policy on using apps, extensions, themes, services, and other add-ons](#)
- [Server log privacy information](#)
- [More information](#)

Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes you can use to change or improve your browsing experience. Privacy practices are different depending on the mode.

you're using.

Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the [network actions prediction](#) feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you've visited before.
- A list of permissions you have granted to websites.
- A searchable index of non-secure pages you visit. Secure (HTTPS) pages, like bank websites, aren't included.
- Thumbnail-sized screenshots of pages you visit most often.
- [Cookies](#) or data from websites you visit.
- Data saved by add-ons.
- A record of what you downloaded from websites.

You can manage this information in several ways:

- You can [delete your browsing history information](#).
- You can clear your cookies and site data by visiting the Cookies and Site Data dialog at `chrome://settings/clearBrowserData`.
- You can stop Chrome from [accepting cookies](#) from Google or other sites. [Learn more](#)

- You can review stored passwords in Chrome settings. [Learn more.](#)
- You can view and manage your stored Autofill information. [Learn more.](#)

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your [Google Account](#) by signing in to Chrome. Signing in enables Chrome's [synchronization feature](#).

How Chrome handles your information

Information for website operators. Sites that you visit using Chrome will automatically receive [standard log information](#), including your system's IP address and data from [cookies](#) or [similar technologies](#). In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that connection to Google or the website you visited to help determine the extent of the attack and how the attack functions. Google provides participating website owners with reports about attacks occurring on their sites.

Prerendering. To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site is allowed to set and read its own cookies just as if you had visited it, even if you don't end up visiting the prerendered page. [Learn more.](#)

Location. To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; however, on mobile devices, once you've granted the app permission to access your location, Chrome automatically shares your location with your default search engine. Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The wi-fi routers closest to you
- Cell IDs of the cell towers closest to you

- The strength of your wi-fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

Updates. Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active users.

Search features. When you search using the address bar in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. This allows your search engine to improve your searching and browsing experience by automatically suggesting terms or URLs you may be looking for. [Learn more](#). If Google is your default search engine, Chrome contacts Google when you start searching or when you change networks, so you can get the best local web address for sending search queries. If you are signed in to a Google site or signed in to Chrome and Google is your default search engine, searches you perform using the address bar in Chrome are stored in your Google account.

Suggestion service. Suggestions are based on related web searches, your browsing history, and popular websites. If your default search engine provides a suggestion service, the browser sends the text you type in the address bar to the search engine. [Learn more about the address bar prediction service](#).

Navigation assistance. When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

Autofill and password management. Chrome sends Google limited, anonymous information about the web forms that you encounter, including a hashed URL of the web page and details of the form's structure, so that we can improve our Autofill and password management services. Some web forms handled by Chrome will offer you the option of Autofilling with cards from Google Payments. If you use a card from Google Payments or choose to save your credit card in your Google Payments account for future use, Chrome will collect information about your computer and share it with Google Payments to protect you from fraud.

Usage statistics and crash reports. You can send usage statistics and crash reports to Google to help us improve our products. For users on our early release versions and on Chromebooks, usage statistics and crash

reports are enabled by default. Usage statistics contain information such as preferences, button clicks, and memory usage. Usage statistics do not include web page URLs or personal information unless you have reached what seems to be a [phishing or malware web page](#). Crash reports contain system information at the time of the crash, and may contain web page URLs or personal information, depending on what was happening at the time the crash report was triggered. We might share aggregated, non-personal information from crash reports with third parties. [Learn more](#).

Content licensing. To allow certain content to be accessed using Chrome browser for Windows or Chrome OS, Chrome provides a unique identifier to content partners and websites that use Adobe Flash Access. The identifier is stored on your system. You can disable this in Chrome settings, or reset the unique identifier's value by reinstalling the operating system. If you access HD content on Chrome OS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. To verify your device, your Chromebook will [share data about its hardware attributes](#) with the website, and will use [Verified Access](#) to certify that its cryptographic keys are protected by Chrome hardware. Chrome will prompt you to allow or deny this verification check. [Learn more](#).

Other Google services. This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You will be notified of your options for controlling these services when you first use them. You can find more information in the [Chrome Privacy Whitepaper](#).

Identifiers in Chrome

Chrome includes a number of identifiers necessary to power features. For example, if you use push messaging, an identifier is created in order to deliver notices to you. Where possible, we use non-unique identifiers and remove identifiers when they are no longer needed. Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome and manage updates.

- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates both a unique token that is sent to Google when you first run and use the browser and, if you received or reactivated your copy of the Chrome browser as part of a promotional campaign, a non-unique promotional tag. Chrome OS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more](#).
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more](#).

Signed-in Chrome mode

When you sign in to the Chrome browser or a Chromebook with your [Google Account](#), your personal browsing data is saved on Google's servers and synced with your account. This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

These settings are automatically loaded for you anytime you sign in to Chrome on other computers and devices. To customize the specific information that you synchronize, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account and manage it on the [Chrome Sync Dashboard](#). On the Dashboard, you can also disable synchronization completely and delete all the associated data from Google's servers. [Learn more](#)

How Chrome handles your signed-in information

When you sync Chrome with your Google Account, we use your browsing data to improve and personalize your experience within Chrome. You can also personalize your experience on other Google products, by allowing your Chrome history to be included in your Google Web & App History. [Learn more](#).

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt all of your synced data with your own sync passphrase. [Learn more.](#)

Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode or guest mode](#). In these modes, Chrome won't store certain information, such as:

- Basic browsing history information like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

How Chrome handles your incognito or guest information

Cookies. Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the incognito or guest window.

Browser configuration changes. When you make changes to your browser configuration, like bookmarking a web page or changing your settings, this information is saved. These changes are not affected by incognito or guest mode.

Permissions. Permissions you grant in incognito mode are not saved to your existing profile.

Profile information. In incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords, while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

Managing Users in Chrome

Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system. [Learn more](#).

You can also create a **supervised user** in Chrome with your Google Account. If you do, Google will synchronize and store information about the supervised user, like history and other settings, with your Google Account. You can view this information at chrome.com/manage.

Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first signs in to Chrome or starts browsing without signing in (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for Chrome OS devices. Your administrators may also have the ability to access, monitor, use or disclose data accessed from your managed device.

Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about suspicious websites is sent and received between the browser you are using and Google's servers.

How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive [standard log information](#), including an IP address and [cookies](#).

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. [Learn more](#).

The following Safe Browsing features are specific to Chrome:

- Some versions of Chrome feature Safe Browsing technology that can identify potentially harmful sites and potentially dangerous file types not already known by Google. The full URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.
- Chrome uses Safe Browsing technology to scan your computer periodically, in order to detect unwanted software that prevents you from changing your settings or otherwise interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.
- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware. This data is sent when you close or navigate away from a Safe Browsing warning page. The reports contain various data, like the potentially dangerous file you encountered, the URL and contents of the website, and the URL of the page that directed you to that site.
- If usage statistics are enabled in Chrome and you visit a site that we think could be potentially harmful, certain additional data will be shared with Google, including the full URL that you visited, the "referrer" header sent to that page, and the URL that matched the Safe Browsing list.
- You can always choose to [disable the Safe Browsing feature within Chrome](#).

Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

Managing add-ons

Before installing an add-on, you should review the requested permissions. Add-ons can have permission to do various things, like:

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

From time to time, Google might discover an add-on that poses a security threat, violates the developer terms for Chrome Web Store, or violates other legal agreements, laws, regulations, or policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.

More information

Information that Google receives when you use Chrome is used and protected under the [Google Privacy Policy](#). Information that other website operators and add-on developers receive, including [cookies](#), is subject to the privacy policies of those websites.

Google adheres to several self-regulatory frameworks, including the US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Framework as set forth by the US Department of Commerce. [Learn more](#).

Definitions

Cookies and similar technologies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the website again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Other technologies are used for similar purposes as a cookie on other platforms where cookies are not available or applicable, such as the Advertising ID available on Android mobile devices. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address and a password). This account information will be used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or terminate your account at any time through your Google Account settings.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry where the search is for "cars", followed by a breakdown of its parts:

123.45.67.89 - 25/Mar/2003 10:15:32 -

<https://www.google.com/search?q=cars> -

Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969

- **123.45.67.89** is the Internet Protocol address assigned to the user by the user's ISP; depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet;
- **25/Mar/2003 10:15:32** is the date and time of the query;
- **<https://www.google.com/search?q=cars>** is the requested URL, including the search query;
- **Firefox 1.0.7; Windows NT 5.1** is the browser and operating system being used, and
- **740674ce2123a969** is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time s/he visited Google, then it will be the unique cookie ID assigned to the user the next time s/he visits Google from that particular computer).

EXHIBIT 115

**8/30/16
CHROME
PRIVACY
NOTICE**

Google Chrome Privacy Notice

Archive date: August 30, 2016

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, Chrome OS, and Safe Browsing. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#).

If you enable Google Play apps on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the Play Terms of Service and Google Privacy Policy. Details specific to Chrome are provided in this Notice where relevant.

Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll call it out.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.

For step-by-step guides to managing your privacy preferences, read [this overview of Chrome's privacy controls](#).

Table of contents:

- [Browser modes](#)
- [Managing users in Chrome](#)
- [Safe Browsing policies](#)
- [Policy on using apps, extensions, themes, services, and other add-ons](#)
- [Server log privacy information](#)
- [More information](#)

Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes you can use to change or improve your browsing experience. Privacy practices are different depending on the mode you're using.

Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the [network actions prediction](#) feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you visit.
- A list of permissions you have granted to websites.
- Thumbnail-sized screenshots of pages you visit most often.
- [Cookies](#) or data from websites you visit.
- Data saved by add-ons.
- A record of what you downloaded from websites.

You can manage this information in several ways:

- You can [delete your browsing history information](#).
- You can clear your cookies and site data by visiting the Cookies and Site Data dialog at <chrome://settings/clearBrowserData>.

- You can stop Chrome from accepting cookies from Google or other sites. [Learn more](#).
- You can review stored passwords in Chrome settings. [Learn more](#).
- You can view and manage your stored Autofill information. [Learn more](#).

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your [Google Account](#) by signing in to Chrome. Signing in enables Chrome's [synchronization feature](#).

How Chrome handles your information

Information for website operators. Sites that you visit using Chrome will automatically receive [standard log information](#), including your system's IP address and data from [cookies](#) or [similar technologies](#). In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that connection to Google or the website you visited to help determine the extent of the attack and how the attack functions. Google provides participating website owners with reports about attacks occurring on their sites.

Prerendering. To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site is allowed to set and read its own cookies just as if you had visited it, even if you don't end up visiting the prerendered page. [Learn more](#).

Location. To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; however, on mobile devices, once you've granted the app permission to access your location, Chrome automatically shares your location with your default search engine. Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The wi-fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your wi-fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

Updates. Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active users.

Search features. When you search using the address bar in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. This allows your search engine to improve your searching and browsing experience by automatically suggesting terms or URLs you may be looking for. [Learn more](#). If Google is your default search engine, Chrome contacts Google when you start searching or when you change networks, so you can get the best local web address for sending search queries. If you are signed in to a Google site or signed in to Chrome and Google is your default search engine, searches you perform using the address bar in Chrome are stored in your Google account.

Suggestion service. Suggestions are based on related web searches, your browsing history, and popular websites. If your default search engine provides a suggestion service, the browser sends the text you type in the address bar to the search engine. [Learn more about the address bar prediction service](#).

Navigation assistance. When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

Autofill and password management. Chrome sends Google limited, anonymous information about the web forms that you encounter, including a hashed URL of the web page and details of the form's structure, so that we can improve our Autofill and password management services.

Payments. If you are signed in to the Chrome browser and you have credit cards stored in your Google Payments Account, then Chrome will offer you the option of filling those cards into web forms. In addition, if you enter a new credit card into a web form, Chrome will offer to save your credit card and related billing

Information to your Google Payments account. If you use a card from Google Payments or choose to save your credit card in your Google Payments account for future use, Chrome will collect information about your computer and share it with Google Payments to protect you from fraud. On Android, if supported by the merchant, Chrome will also allow you to pay using Android Pay.

Usage statistics and crash reports. You can send usage statistics and crash reports to Google to help us improve our products. For users on our early release versions and on Chromebooks, usage statistics and crash reports are enabled by default. Usage statistics contain information such as preferences, button clicks, and memory usage. Usage statistics do not include web page URLs or personal information unless you have reached what seems to be a [phishing or malware web page](#). Crash reports contain system information at the time of the crash, and may contain web page URLs or personal information, depending on what was happening at the time the crash report was triggered. We might share aggregated, non-personal information from crash reports with third parties. [Learn more](#). If Google Play apps are enabled on your Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.

Content licensing. To allow certain content to be accessed using Chrome browser for Windows or Chrome OS, Chrome provides a unique identifier to content partners and websites that use Adobe Flash Access. The identifier is stored on your system. You can disable this in Chrome settings, or reset the unique identifier's value by reinstalling the operating system. If you access HD content on Chrome OS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. To verify your device, your Chromebook will [share data about its hardware attributes](#) with the website, and will use [Verified Access](#) to certify that its cryptographic keys are protected by Chrome hardware. Chrome will prompt you to allow or deny this verification check. [Learn more](#).

Other Google services. This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You will be notified of your options for controlling these services when you first use them. You can find more information in the [Chrome Privacy Whitepaper](#).

Identifiers in Chrome

Chrome includes a number of identifiers necessary to power features. For example, if you use push messaging, an identifier is created in order to deliver notices to you. Where possible, we use non-unique identifiers and

remove identifiers when they are no longer needed. Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome.
- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates both a unique token that is sent to Google when you first run and use the browser and, if you received or reactivated your copy of the Chrome browser as part of a promotional campaign, a non-unique promotional tag. Chrome OS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more](#)
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more](#).

Signed-in Chrome mode

When you sign in to the Chrome browser or a Chromebook with your [Google Account](#), your personal browsing data is saved on Google's servers and synced with your account. This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

These settings are automatically loaded for you anytime you sign in to Chrome on other computers and devices. To customize the specific information that you synchronize, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account and manage it on the [Chrome Sync](#)

Dashboard. On the Dashboard, you can also disable synchronization completely and delete all the associated data from Google's servers. [Learn more](#).

How Chrome handles your signed-in information

When you sync Chrome with your Google Account, we use your browsing data to improve and personalize your experience within Chrome. You can also personalize your experience on other Google products, by allowing your Chrome history to be included in your Google Web & App Activity. [Learn more](#).

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt all of your synced data with your own sync passphrase. [Learn more](#).

Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode or guest mode](#). In these modes, Chrome won't store certain information, such as:

- Basic browsing history information like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

How Chrome handles your incognito or guest information

Cookies. Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.

Browser configuration changes. When you make changes to your browser configuration, like bookmarking a web page or changing your settings, this information is saved. These changes are not affected by incognito or

guest mode.

Permissions. Permissions you grant in incognito mode are not saved to your existing profile.

Profile information. In incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords, while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

Managing Users in Chrome

Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system. [Learn more.](#)

You can also create a [**supervised user**](#) in Chrome with your Google Account. If you do, Google will synchronize and store information about the supervised user, like history and other settings, with your Google Account. You can view this information at chrome.com/manage.

Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first signs in to Chrome or starts browsing without signing in (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for Chrome OS devices. Your administrators may also have the ability to access, monitor, use or disclose data accessed from your managed device.

Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about suspicious websites is sent and received between the browser you are using and Google's servers.

How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive [standard log information](#), including an IP address and [cookies](#).

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. [Learn more](#).

The following Safe Browsing features are specific to Chrome:

- Some versions of Chrome feature Safe Browsing technology that can identify potentially harmful sites and potentially dangerous file types not already known by Google. The full URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.
- Chrome uses Safe Browsing technology to scan your computer periodically, in order to detect unwanted software that prevents you from changing your settings or otherwise interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.
- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware. This data is sent when you close or navigate away from a Safe Browsing warning page. The reports contain various data, like the potentially dangerous file you encountered, the URL and contents of the website, and the URL of the page that directed you to that site.

- If usage statistics are enabled in Chrome and you visit a site that we think could be potentially harmful, certain additional data will be shared with Google, including the full URL that you visited, the "referrer" header sent to that page, and the URL that matched the Safe Browsing list.
 - You can always choose to [disable the Safe Browsing feature within Chrome](#).
-

Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

Managing add-ons

Before installing an add-on, you should review the requested permissions. Add-ons can have permission to do various things, like:

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

From time to time, Google might discover an add-on that poses a security threat, violates the developer terms for Chrome Web Store, or violates other legal agreements, laws, regulations, or policies. Chrome periodically

downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.

More information

Information that Google receives when you use Chrome is used and protected under the [Google Privacy Policy](#). Information that other website operators and add-on developers receive, including [cookies](#), is subject to the privacy policies of those websites.

Google adheres to several self-regulatory frameworks, including the US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Framework as set forth by the US Department of Commerce. [Learn more](#).

Definitions

Cookies and similar technologies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the website again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Other technologies are used for similar purposes as a cookie on other platforms where cookies are not available or applicable, such as the Advertising ID available on Android mobile devices. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address and a password). This account information will be used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or terminate your account at any time through your Google Account settings.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry where the search is for "cars", followed by a breakdown of its parts:

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
https://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 - 740674ce2123a969
```

- **123.45.67.89** is the Internet Protocol address assigned to the user by the user's ISP; depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet;
- **25/Mar/2003 10:15:32** is the date and time of the query;
- **https://www.google.com/search?q=cars** is the requested URL, including the search query;
- **Firefox 1.0.7; Windows NT 5.1** is the browser and operating system being used; and
- **740674ce2123a969** is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time s/he visited Google, then it will be the unique cookie ID assigned to the user the next time s/he visits Google from that particular computer).

EXHIBIT 116

**10/11/16
CHROME
PRIVACY
NOTICE**

Google Chrome Privacy Notice

Archive date: October 11, 2016

Learn how to control the information that's collected, stored, and shared when you use the Google Chrome browser on your computer or mobile device, Chrome OS, and Safe Browsing. Although this policy describes features that are specific to Chrome, any personal information that is provided to Google or stored in your Google Account will be used and protected in accordance with the [Google Privacy Policy](#).

If you enable Google Play apps on your Chromebook, the use and protection of information collected by Google Play or the Android operating system is governed by the Play Terms of Service and Google Privacy Policy. Details specific to Chrome are provided in this Notice where relevant.

Details about the Privacy Notice

In this Privacy Notice, we use the term "Chrome" to refer to all the products in the Chrome family listed above. If there are differences in our policy between products, we'll point them out.

"Beta," "Dev," or "Canary" versions of Chrome let you test new features still being created in Chrome. This Privacy Notice applies to all versions of Chrome, but might not be up-to-date for features still under development.

For step-by-step guides to managing your privacy preferences, read [this overview of Chrome's privacy controls](#).

Table of contents:

- [Browser modes](#)
- [Managing users in Chrome](#)
- [Safe Browsing policies](#)
- [Policy on using apps, extensions, themes, services, and other add-ons](#)
- [Server log privacy information](#)
- [More information](#)

Browser modes

You don't need to provide any personal information to use Chrome, but Chrome has different modes that you can use to change or improve your browsing experience. Privacy practices are different depending on the mode that you're using.

Basic browser mode

The basic browser mode stores information locally on your system. This information might include:

- Browsing history information. For example, Chrome stores the URLs of pages that you visit, a cache of text, images and other resources from those pages, and, if the [network actions prediction](#) feature is turned on, a list of some of the IP addresses linked from those pages.
- Personal information and passwords, to help you fill out forms or sign in to sites you visit.
- A list of permissions that you have granted to websites.
- Thumbnail-sized screenshots of pages that you visit most often.
- [Cookies](#) or data from websites that you visit.
- Data saved by add-ons.
- A record of what you downloaded from websites.

You can manage this information in several ways:

- You can [delete your browsing history information](#).
- You can clear your cookies and site data by visiting the Cookies and Site Data dialog at <chrome://settings/clearBrowserData>.

- You can stop Chrome from accepting cookies from Google or other sites. [Learn more](#).
- You can review stored passwords in Chrome settings. [Learn more](#).
- You can view and manage your stored Autofill information. [Learn more](#).

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your [Google Account](#) by signing in to Chrome. Signing in enables Chrome's [synchronization feature](#).

How Chrome handles your information

Information for website operators. Sites that you visit using Chrome will automatically receive [standard log information](#), including your system's IP address and data from [cookies](#) or [similar technologies](#). In general, the fact that you use Chrome to access Google services, such as Gmail, does not cause Google to receive any additional personally identifying information about you. On Google websites and other websites that opt in, if Chrome detects signs that you are being actively attacked by someone on the network (a "man in the middle attack"), Chrome may send information about that connection to Google or the website you visited to help determine the extent of the attack and how the attack functions. Google provides participating website owners with reports about attacks occurring on their sites.

Prerendering. To load web pages faster, Chrome has a setting that can look up the IP addresses of links on a web page and open network connections. Sites and Android apps can also ask the browser to preload the pages you might visit next. Preloading requests from Android apps are controlled by the same setting as Chrome-initiated predictions. But preloading instructions from sites are always performed, regardless of whether Chrome's network prediction feature is enabled. If prerendering is requested, whether by Chrome or by a site or app, the preloaded site is allowed to set and read its own cookies just as if you had visited it, even if you don't end up visiting the prerendered page. [Learn more](#).

Location. To get more geographically relevant information, Chrome gives you the option to share your location with a site. Chrome won't allow a site to access your location without your permission; however, on mobile devices, once you've granted the app permission to access your location, Chrome automatically shares your location with your default search engine. Chrome uses Google Location Services to estimate your location. The information that Chrome sends to Google Location Services may include:

- The Wi-Fi routers closest to you
- Cell IDs of the cell towers closest to you
- The strength of your Wi-Fi or cell signal
- The IP address that is currently assigned to your device

Google doesn't have control over third-party websites or their privacy practices, so be cautious when sharing your location with a website.

Updates. Chrome periodically sends information to Google to check for updates, get connectivity status, validate the current time, and estimate the number of active users.

Search features. When you search using the address bar in Chrome, the characters you type (even if you haven't hit "enter" yet) are sent to your default search engine. This allows your search engine to improve your searching and browsing experience by automatically suggesting terms or URLs you may be looking for. [Learn more](#). If Google is your default search engine, Chrome contacts Google when you start searching or when you change networks, so you can get the best local web address for sending search queries. If you are signed in to a Google site or signed in to Chrome and Google is your default search engine, searches you perform using the address bar in Chrome are stored in your Google account.

Suggestion service. Suggestions are based on related web searches, your browsing history, and popular websites. If your default search engine provides a suggestion service, the browser sends the text you type in the address bar to the search engine. [Learn more about the address bar prediction service](#).

Navigation assistance. When you can't connect to a web page, you can get suggestions for alternative pages similar to the one you're trying to reach. In order to offer you suggestions, Chrome sends Google the URL of the page you're trying to reach.

Autofill and password management. Chrome sends Google limited, anonymous information about the web forms that you encounter, including a hashed URL of the web page and details of the form's structure, so that we can improve our Autofill and password management services.

Payments. If you are signed in to the Chrome browser and you have credit cards stored in your Google Payments Account, then Chrome will offer you the option of filling those cards into web forms. In addition, if you enter a new credit card into a web form, Chrome will offer to save your credit card and related billing

Information to your Google Payments account. If you use a card from Google Payments or choose to save your credit card in your Google Payments account for future use, Chrome will collect information about your computer and share it with Google Payments to protect you from fraud. On Android, if supported by the merchant, Chrome will also allow you to pay using Android Pay.

Usage statistics and crash reports. By default, usage statistics and crash reports are sent to Google to help us improve our products. Usage statistics contain information such as preferences, button clicks, and memory usage. Usage statistics do not include web page URLs or personal information. Crash reports contain system information at the time of the crash, and may contain web page URLs or personal information, depending on what was happening at the time the crash report was triggered. We might share aggregated, non-personal information from crash reports with third parties. You can change whether usage statistics and crash reports are sent to Google at any time. [Learn more](#). If Google Play apps are enabled on your Chromebook and Chrome usage statistics are enabled, then Android diagnostic and usage data is also sent to Google.

Content licensing. To allow certain content to be accessed using Chrome browser for Windows or Chrome OS, Chrome provides a unique identifier to content partners and websites that use Adobe Flash Access. The identifier is stored on your system. You can disable this in Chrome settings, or reset the unique identifier's value by reinstalling the operating system. If you access HD content on Chrome OS, a content provider may ask Chrome for a certificate to verify the eligibility of the device. To verify your device, your Chromebook will [share data about its hardware attributes](#) with the website, and will use [Verified Access](#) to certify that its cryptographic keys are protected by Chrome hardware. Chrome will prompt you to allow or deny this verification check. [Learn more](#).

Other Google services. This notice describes the Google services that are enabled by default in Chrome. In addition, Chrome may offer other Google web services. For example, if you encounter a page in a different language, Chrome will offer to send the text to Google for translation. You will be notified of your options for controlling these services when you first use them. You can find more information in the [Chrome Privacy Whitepaper](#).

Identifiers in Chrome

Chrome includes a number of identifiers necessary to power features. For example, if you use push messaging, an identifier is created in order to deliver notices to you. Where possible, we use non-unique identifiers and

remove identifiers when they are no longer needed. Additionally, the following identifiers help us develop, distribute, and promote Chrome, but are not directly related to a Chrome feature.

- **Installation tracking.** Each copy of the Windows desktop version of the Chrome browser includes a temporary randomly generated installation number that is sent to Google when you install and first use Chrome. This temporary identifier helps us estimate the number of installed browsers, and will be deleted the first time Chrome updates. The mobile version of Chrome uses a variant of the device identifier on an ongoing basis to track the number of installations of Chrome.
- **Promotion tracking.** In order to help us track the success of promotional campaigns, Chrome generates a unique token that is sent to Google when you first run and use the browser. In addition, if you received or reactivated your copy of the desktop version of the Chrome browser as part of a promotional campaign and Google is your default search engine, then searches from the omnibox will include a non-unique promotional tag. All mobile versions of the Chrome browser also include a non-unique promotional tag with searches from the omnibox. Chrome OS may also send a non-unique promotional tag to Google periodically (including during initial setup) and when performing searches with Google. [Learn more](#).
- **Field trials.** We sometimes conduct limited tests of new features. Chrome includes a seed number that is randomly selected on first run to assign browsers to experiment groups. Experiments may also be limited by country (determined by your IP address), operating system, Chrome version, and other parameters. A list of field trials that are currently active on your installation of Chrome is included in all requests sent to Google. [Learn more](#).

Signed-in Chrome mode

When you sign in to the Chrome browser or a Chromebook with your [Google Account](#), your personal browsing data is saved on Google's servers and synced with your account. This type of information can include:

- Browsing history
- Bookmarks
- Tabs
- Passwords and Autofill information
- Other browser settings, like installed extensions

These settings are automatically loaded for you anytime you sign in to Chrome on other computers and devices. To customize the specific information that you synchronize, use the "Settings" menu. [Learn more](#). You can see the amount of Chrome data stored for your Google Account and manage it on the [Chrome Sync Dashboard](#). On the Dashboard, you can also disable synchronization completely and delete all the associated data from Google's servers. [Learn more](#).

How Chrome handles your signed-in information

When you sync Chrome with your Google Account, we use your browsing data to improve and personalize your experience within Chrome. You can also personalize your experience on other Google products, by allowing your Chrome history to be included in your Google Web & App Activity. [Learn more](#).

You can change this setting on your [Account History](#) page or [manage your private data](#) whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users. Google uses this data to develop new features, products, and services, and to improve the overall quality of existing products and services. If you would like to use Google's cloud to store and sync your Chrome data but you don't want Google to access the data, you can encrypt all of your synced data with your own sync passphrase. [Learn more](#).

Incognito mode and guest mode

You can limit the information Chrome stores on your system by using [incognito mode or guest mode](#). In these modes, Chrome won't store certain information, such as:

- Basic browsing history information like URLs, cached page text, or IP addresses of pages linked from the websites you visit
- Snapshots of pages that you visit
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device

How Chrome handles your incognito or guest information

Cookies. Chrome won't share existing cookies with sites you visit in incognito or guest mode. Sites may deposit new [cookies](#) on your system while you are in these modes, but they'll only be stored and transmitted until you close the last incognito or guest window.

Browser configuration changes. When you make changes to your browser configuration, like bookmarking a web page or changing your settings, this information is saved. These changes are not affected by incognito or guest mode.

Permissions. Permissions you grant in incognito mode are not saved to your existing profile.

Profile information. In incognito mode, you will still have access to information from your existing profile, such as suggestions based on your browsing history and saved passwords, while you are browsing. In guest mode, you can browse without seeing information from any existing profiles.

Managing Users in Chrome

Managing users for personal Chrome use

You can set up personalized versions of Chrome for users sharing one device or computer. Note that anyone with access to your device can view all the information in all profiles. To truly protect your data from being seen by others, use the built-in user accounts in your operating system. [Learn more](#).

You can also create a [supervised user](#) in Chrome with your Google Account. If you do, Google will synchronize and store information about the supervised user, like history and other settings, with your Google Account. You can view this information at chrome.com/manage.

Managing users on Chrome for Enterprise

Some Chrome browsers or Chromebooks are managed by a school or company. In that case, the administrator has the ability to apply policies to the browser or Chromebook. Chrome contacts Google to check for these policies when a user first signs in to Chrome or starts browsing without signing in (except in guest mode). Chrome checks periodically for updates to policies.

An administrator can set up a policy for status and activity reporting for Chrome, including location information for Chrome OS devices. Your administrators may also have the ability to access, monitor, use or disclose data accessed from your managed device.

Safe Browsing practices

Google Chrome and certain third-party browsers, like some versions of Mozilla Firefox and Apple's Safari, include Google's Safe Browsing feature. With Safe Browsing, information about suspicious websites is sent and received between the browser you are using and Google's servers.

How Safe Browsing works

Your browser contacts Google's servers periodically to download the most recent "Safe Browsing" list, which contains known phishing and malware sites. The most recent copy of the list is stored locally on your system. Google doesn't collect any account information or other personally identifying information as part of this contact. However, it does receive [standard log information](#), including an IP address and [cookies](#).

Each site you visit is checked against the Safe Browsing list on your system. If there's a match, your browser sends Google a hashed, partial copy of the site's URL so that Google can send more information to your browser. Google cannot determine the real URL from this information. [Learn more](#).

The following Safe Browsing features are specific to Chrome:

- Some versions of Chrome feature Safe Browsing technology that can identify potentially harmful sites and potentially dangerous file types not already known by Google. The full URL of the site or potentially dangerous file might also be sent to Google to help determine whether the site or file is harmful.
- Chrome uses Safe Browsing technology to scan your computer periodically, in order to detect unwanted software that prevents you from changing your settings or otherwise interferes with the security and stability of your browser. [Learn more](#). If this kind of software is detected, Chrome might offer you the option to download the [Chrome Cleanup Tool](#) to remove it.
- You can choose to send additional data to help improve Safe Browsing when you access a site that appears to contain malware. This data is sent when you close or navigate away from a Safe Browsing warning page. The reports contain various data, like the potentially dangerous file you encountered, the URL and contents of the website, and the URL of the page that directed you to that site.

- If you are a Safe Browsing user and you are syncing your Chrome browsing history to your Google account, then, to improve the safety and utility of web feature permissions, Chrome may anonymously report the domains on which you grant, reject, and revoke permissions, or ignore or dismiss permission prompts.
 - You can always choose to [disable the Safe Browsing feature within Chrome](#).
-

Privacy practices of apps, extensions, themes, services, and other add-ons

You can use apps, extensions, themes, services and other add-ons with Chrome, including some that may be preinstalled or integrated with Chrome. Add-ons developed and provided by Google may communicate with Google servers and are subject to the [Google Privacy Policy](#) unless otherwise indicated. Add-ons developed and provided by others are the responsibility of the add-on creators and may have different privacy policies.

Managing add-ons

Before installing an add-on, you should review the requested permissions. Add-ons can have permission to do various things, like:

- Store, access, and share data stored locally or in your Google Drive account
- View and access content on websites you visit
- Use notifications that are sent through Google servers

Chrome can interact with add-ons in a few different ways:

- Checking for updates
- Downloading and installing updates
- Sending usage indicators to Google about the add-ons

Some add-ons might require access to a unique identifier for digital rights management or for delivery of push messaging. You can disable the use of identifiers by removing the add-on from Chrome.

From time to time, Google might discover an add-on that poses a security threat, violates the developer terms for Chrome Web Store, or violates other legal agreements, laws, regulations, or policies. Chrome periodically downloads a list of these dangerous add-ons, in order to remotely disable or remove them from your system.

More information

Information that Google receives when you use Chrome is used and protected under the [Google Privacy Policy](#). Information that other website operators and add-on developers receive, including [cookies](#), is subject to the privacy policies of those websites.

Google adheres to several self-regulatory frameworks, including the US-EU Safe Harbor Framework and the US-Swiss Safe Harbor Framework as set forth by the US Department of Commerce. [Learn more](#).

Definitions

Cookies and similar technologies

A cookie is a small file containing a string of characters that is sent to your computer when you visit a website. When you visit the website again, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies. Other technologies are used for similar purposes as a cookie on other platforms where cookies are not available or applicable, such as the Advertising ID available on Android mobile devices. Learn more about [how Google uses cookies](#) and how Google uses data, including cookies, [when you use our partners' sites or apps](#).

Google Account

You may access some of our services by signing up for a [Google Account](#) and providing us with some personal information (typically your name, email address and a password). This account information will be used to authenticate you when you access Google services and protect your account from unauthorized access by others. You can edit or terminate your account at any time through your Google Account settings.

Server logs

Like most websites, our servers automatically record the page requests made when you visit our sites. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Here is an example of a typical log entry where the search is for "cars", followed by a breakdown of its parts.

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
https://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969
```

- **123.45.67.89** is the Internet Protocol address assigned to the user by the user's ISP; depending on the user's service, a different address may be assigned to the user by their service provider each time they connect to the Internet;
- **25/Mar/2003 10:15:32** is the date and time of the query;
- **https://www.google.com/search?q=cars** is the requested URL, including the search query;
- **Firefox 1.0.7; Windows NT 5.1** is the browser and operating system being used, and
- **740674ce2123a969** is the unique cookie ID assigned to this particular computer the first time it visited Google. (Cookies can be deleted by users. If the user has deleted the cookie from the computer since the last time s/he visited Google, then it will be the unique cookie ID assigned to the user the next time s/he visits Google from that particular computer).